Microsoft

A Cloud for Global Good

Navigating your way to the cloud in healthcare

A practical guide for the healthcare industry in the Philippines

The Digital Transformation of Healthcare in the Philippines

The Philippines is undergoing a rapid transformation powered by new technologies. In a market with 45 million internet users and increasing support from policy and regulation, organizations across the country are looking to harness new technologies to empower their people to achieve more.

The healthcare industry, more than almost any other, is being transformed by these developments. Healthcare institutions[1] in the Philippines are deploying digital platforms and services to optimise clinical and operational effectiveness, empower care teams, engage with patients and raise the quality of care.

To a large extent, the digital transformation of healthcare that is happening in the Philippines and around the world is powered by cloud technologies. Cloud computing holds the promise to drive enormous societal and economic benefits at an unprecedented scale and pace. At Microsoft, we believe that to ensure the benefits of cloud computing are broadly shared, a balanced set of policy and technology solutions that will promote positive change is necessary. The Philippines' experience exemplifies this. The Department of Health, working with the Department of Science, has implemented various initiatives to deliver the Philippines eHealth Vision by 2020. Meanwhile, the "cloud-first" policy issued by the Department of Information and Communications Technology in 2017 provides top-down support for the use of cloud technologies to reduce costs, increase productivity and improve services.

Despite the progress, there are still enormous opportunities for future growth in the use of cloud services by healthcare institutions in the Philippines. In the past, the pace of cloud adoption in the Philippines' healthcare industry was slower than in other sectors, largely because of concerns about the regulatory environment. Whilst matters such data privacy and data security remain at the core of the healthcare regulatory environment in the Philippines and must be addressed as part of any technology adoption, there is now widespread acceptance that cloud services have the potential to comply with (and even enhance the level of compliance with) the necessary regulatory requirements in the Philippines.

At Microsoft, the positive outlook for the healthcare industry in the Philippines inspires us. Having partnered with organisations across all sectors in the Philippines for many years, we have witnessed the transformational power of technology in the country. This paper is a further contribution to the digital transformation of the Philippines' healthcare industry. Designed as a practical roadmap, it will help the Philippines' healthcare institutions take full advantage of the transformational benefits of cloud technologies based on a full understanding of the regulatory framework. We also share examples of how cloud technologies are already transforming the way healthcare services are provided in the Philippines.

We hope this paper is useful and look forward to continuing the conversation as we seek to realise our mission of helping the Philippines' healthcare institutions in their journey towards a digital future. We are committed to ensuring that healthcare institutions in the country and their patients will benefit from this new wave of innovation. Delivering a cloud that is trusted, responsible and inclusive is a key part of our commitment to this digital transformation and to a cloud that serves the global good.

> *"By 2020 eHealth will enable widespread access to health care services, health information, and securely share and exchange patients' information in support to a safer, quality health care, more equitable and responsive health system for all the Filipino people by transforming the way information is used to plan, manage, deliver and monitor health services."*
>
> **The eHealth Vision,**
> Ministry of Health,
> "Philippines eHealth Strategic Framework and Plan", 2013-2017

[1] In this paper, we use the term "healthcare institutions" broadly to refer to the full spectrum of public and private sector healthcare operations in the Philippines.

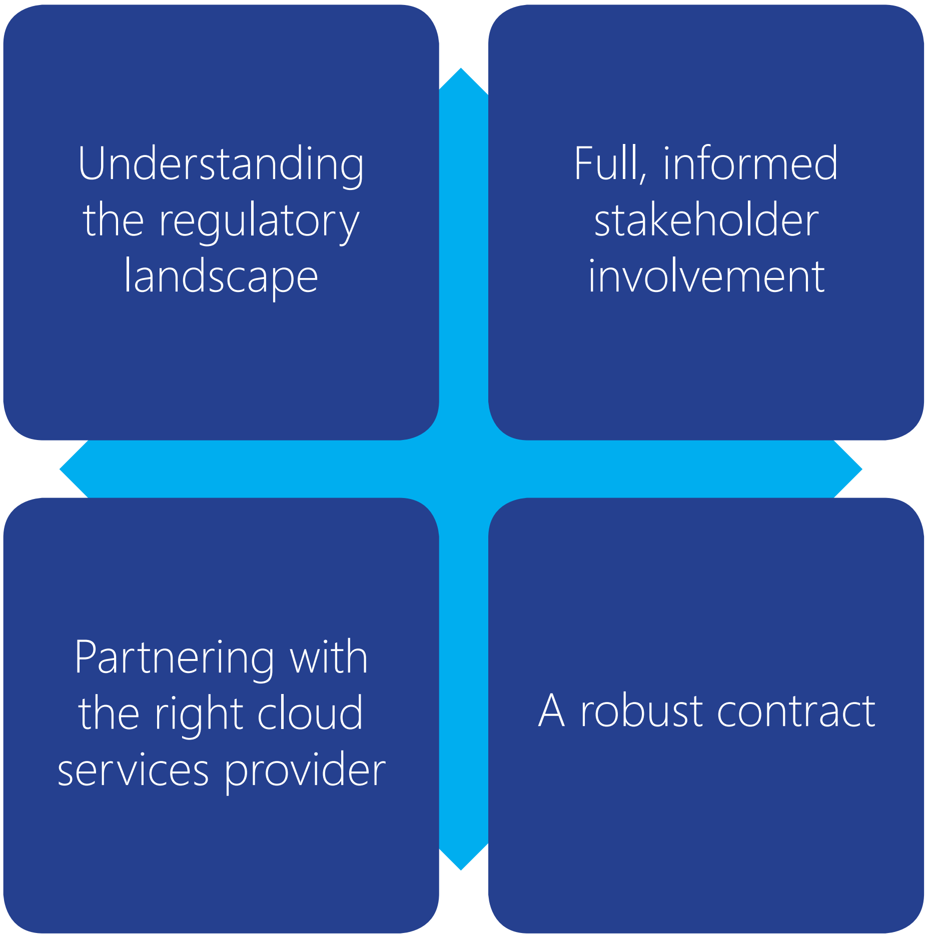
OVERVIEW

The four pillars of a successful cloud adoption

Based on Microsoft's experience of working with healthcare institutions in the Philippines and around the world, a successful cloud adoption rests on four pillars, as shown below.

Importantly, Microsoft recognises that each of these pillars is inter-related and inter-dependent. For example, assurances made by a cloud services provider in response to selection criteria will need to translate into binding commitments set out in a robust contract.

By focusing on these four pillars, healthcare institutions in the Philippines can move to the cloud in a way that addresses the key regulatory and compliance considerations.


Understanding the regulatory landscape
Full, informed stakeholder involvement
Partnering with the right cloud services provider
A robust contract

The following pages describe these pillars in greater detail.

PILLAR 1

Understanding the regulatory landscape

Summary

A successful cloud adoption begins by understanding the regulatory landscape for the adoption of technology by healthcare institutions. We set out below further details of the regulatory environment and the process for cloud adoption in the Philippines, with the goal of making the entire process more streamlined for healthcare institutions.

The regulatory landscape

Are cloud services permitted?	**Yes**.
Who are the relevant regulators and authorities?	• Department of Health (**DOH**) • Department of Information and Communication Technology • National Privacy Commission (**NPC**) • National Telecommunications Commission (**NTC**)
What regulations and guidance are relevant?	• An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes (**DPA**) • Implementing Rules and Regulations of the Data Privacy Act of 2012 (**DPA IRR**) • National Privacy Commission Circular on Personal Data Breach Management (**NPC Circular No. 3 series of 2012**) • An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes (**Cybercrime Prevention Act 2012**) • An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use thereof, and for Other Purposes (**Electronic Commerce Act of 2000**) • Privacy Guidelines for the Implementation of the Philippine Health Information Exchange (**PHIE Privacy Guidelines**) • An Act Promulgating Policies and Prescribing Measures for the Prevention and Control of HIV/AIDS in the Philippines, Instituting a

What regulations and guidance are relevant?	Nationwide HIV/AIDS Information and Educational Program, Establishing a Comprehensive HIV/AIDS Monitoring System, Strengthening the Philippine National Aids Council, and For Other Purposes (**Philippines AIDS Prevention and Control Act 1998**) • An Act to Promote and Govern the Development of Philippine Telecommunications and the Delivery of Public Telecommunications Services (**Public Telecommunications Policy Act**) • National Memorandum Circular on Value Added Services (**MC 2-5-2008**) • DOH-DOST-PHIC Administrative Order No. 2016-0002 Privacy Guidelines in relation to the PHIE (**PHIE Privacy Guidelines**)
Are transfers of data outside of the Philippines permitted?	**Yes**.
Is regulatory approval or registration required?	**No, other than in limited circumstances.** There is a requirement for a government agency to obtain approval from the head of the relevant agency if they wish to access or process sensitive personal information[2] outside of government property. However, in practice, the "cloud-first" policy issued by the Department of Information and Communications Technology requires all government agencies to adopt cloud computing as the preferred ICT deployment strategy, so to the extent approval requirements apply they are not expected to constitute a barrier to the use of cloud services. DPA IRR requires registration with the NPC of any personal data processing system (DPS)[3] that involves accessing sensitive personal information of at least one thousand (1,000) individuals and that is a DPS of a personal information controller[4] or personal information processor[5] that either: (a) employs at least two hundred and fifty (250) persons; or (b) employs fewer than two hundred and fifty (250) persons and carries out processing likely to pose a risk to the rights and freedoms of data subjects or processing that is not occasional. The DPA IRR also requires a personal information controller who carries out any wholly or partly automated processing operations or set of such operations intended to serve a single purpose or several related purposes, to notify the NPC when such automated

[2] "Sensitive personal information" is defined in the DPA as including, amongst others, information about a person's health, race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations.

[3] DPS refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

[4] "Personal information controllers" are defined in the DPA IRR as a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes: (i) natural or juridical persons who perform such functions as instructed by another person or organization; and (ii) natural persons who processes personal data in connection with his or her personal, family, or household affairs.

[5] "Personal information processors" are defined in the DPA IRR as any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject

	processing becomes the sole basis for making decisions about a data subject, and when such decision would significantly affect the data subject. If a healthcare institution involved in the Philippines Health Information Exchange[6] (**PHIE**) wishes to contract with third parties, including cloud services providers, for the sole purpose of processing patient data, it must first get approval from the PHIE Governance Structure in accordance with the PHIE Privacy Guidelines.
Are there any mandatory terms that must be included in the cloud contract with the services provider?	**Yes**. See Pillar 4, below.

How Microsoft helps

Close cooperation with regulators and institutions in relation to a number of successful technology projects in the Philippines has given Microsoft an in-depth understanding of the regulatory framework. Issuing this paper is part of Microsoft's commitment to its healthcare industry customers to help them navigate and comply with the regulatory framework as it applies to cloud services.

In addition to this paper, Microsoft has developed a checklist mapping its compliance against each of the underlying regulatory requirements. For example, if a healthcare institution wishes to understand how Microsoft cloud services comply with the applicable security requirements, they can easily verify this by accessing relevant product and service information. This checklist is available from your Microsoft contact upon request.

To further streamline cloud adoption, Microsoft's team will be on-hand throughout the process to help you with any questions you may have along the way. You can also access the Microsoft Trust Center at microsoft.com/trust, which includes detailed security, privacy, and compliance information for all Microsoft cloud services.

[6] The PHIE is a government project for the collection and sharing of patient data.

PILLAR 2

Full, informed stakeholder involvement

Summary

Microsoft's experience is that a smooth cloud adoption depends on full, informed stakeholder involvement from the outset, with decisions being based on a complete understanding of the proposed cloud solution. Although this is not a specific regulatory requirement, putting the right team in place and understanding all aspects of the proposed technology are essential for the healthcare institution to satisfy itself that the cloud adoption meets the necessary requirements. Microsoft believes that it is the responsibility of the cloud services provider to make available detailed product and service information to ensure that the key decision-makers have all of the materials they need to make an informed choice.

Recommendations

Build the core stakeholder team and develop the business case

A multi-disciplinary team should be put in place by the healthcare institution from day one:

- The institution's technology and procurement teams should take the lead in developing the business case, with a focus on the operational, commercial and patient care factors driving the decision to adopt cloud services.
- The institution's legal, risk and compliance teams should be involved in these discussions from the outset, to map the proposed solutions against legal and regulatory requirements and to build in the necessary timeframes to engage with regulators. Many technology projects have been delayed by involving the legal, risk and compliance functions too late in the process.
- The institution's board and senior management will typically require early reassurance in general terms regarding the business need for the use of cloud services and the oversight, review, reporting and response arrangements to be put in place with the cloud services provider.

Understand the technical solutions available

Any healthcare institution's technology procurement project requires that all of its key decision-makers have a full understanding of the technology solution to be deployed.

This begins by ensuring that every member of the core team has a clear understanding of the proposed cloud service and deployment models. A range of options exists, including public, private, hybrid and community cloud, but given the operational and commercial benefits to customers, public cloud is increasingly seen as the standard deployment model for most institutions.

You can access more information about the service and deployment models on offer through the Microsoft Trust Center at microsoft.com/trust.

Obtain detailed product and service information	Having understood the technical solutions at a high-level, the healthcare institution should also obtain detailed product and service information from the cloud services provider. It is important to have a detailed understanding of the cloud solution to ensure that it meets the relevant regulatory requirements. We expand on this in the next pillar, “Partnering with the right cloud services provider“.

How Microsoft helps

A digital transformation is a journey. Like all journeys, we must know where we are starting from, and we must have a destination in mind.

Microsoft’s expert team is on hand to support you throughout your cloud project, right from the earliest stages of initial stakeholder engagement through to the rollout of the solution. Our cloud product range spans all cloud service and deployment models and, with our Japan-based data centers and transparent approach to data location, we provide cloud customers with the flexibility to decide how and where their data will be stored and processed. We have developed a range of materials, including product fact sheets and online trust centers, designed to ensure that you have access to all the information needed to make an informed decision. Our subject-matter experts are available to meet with you and your core stakeholders to provide specific and detailed information on the technical, contractual and practical aspects of your proposed cloud project.

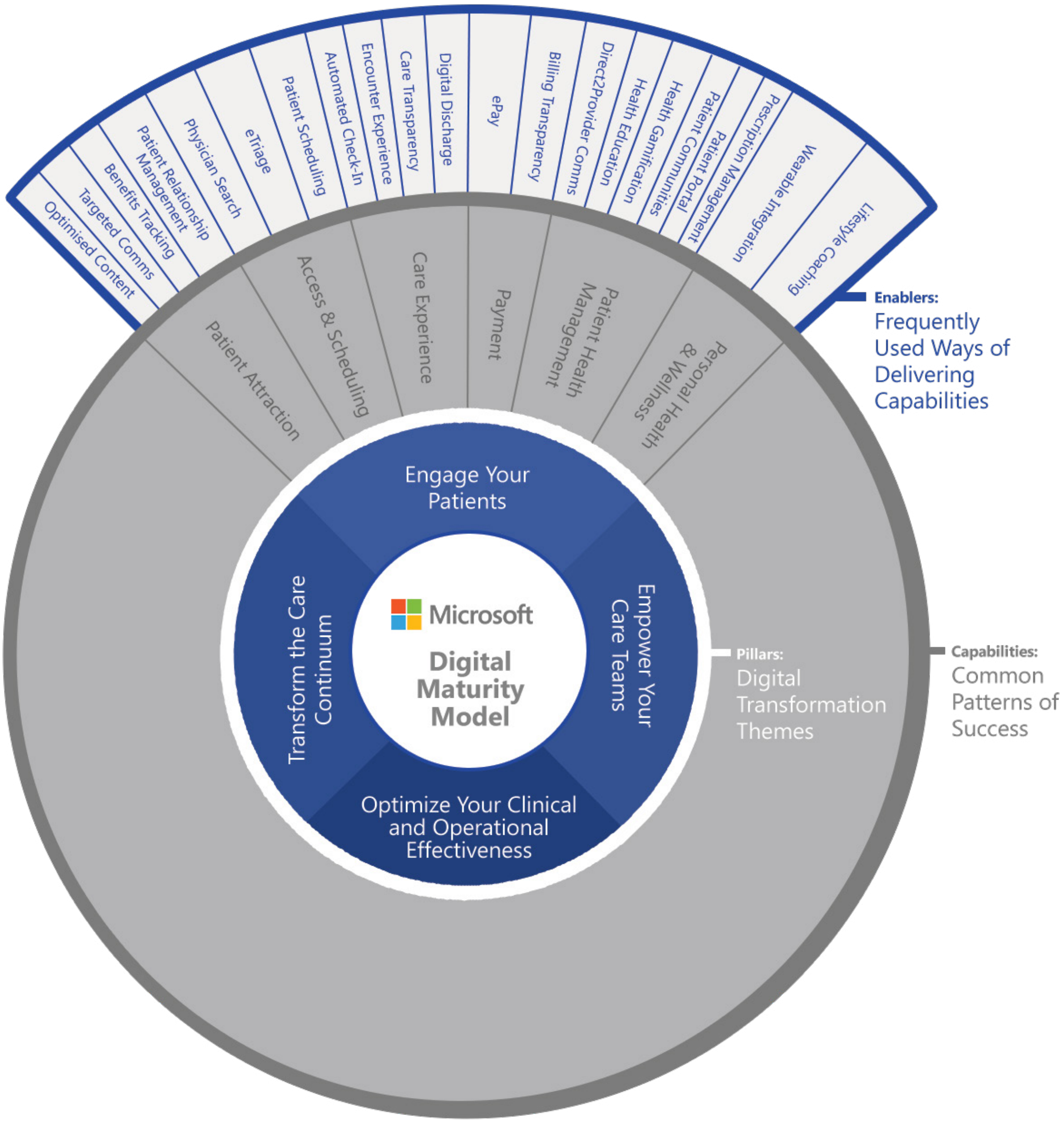
For healthcare providers seeking end-to-end advice and support in relation to transformative digital projects, we have developed the Digital Maturity Model (DMM). Developed in association with healthcare practice leads and subject matter experts from McKinsey, as well as Microsoft’s own subject matter experts, the DMM is designed to help our customers focus on the components of a digital transformation that are most likely to have the greatest impact.

The DMM allows for the evaluation of where customers are in their digital transformation journey by examining their efforts across four key pillars:

- **Engage your patients:** patient-centric delivery to get patients healthy and help them stay healthy;
- **Empower your care teams:** applying digital capabilities to improve care team productivity;
- **Optimise your clinical and operational effectiveness:** using digitised processes to drive better diagnoses and treatment; and
- **Transform the care continuum:** redefining care delivery through platforms that provide insight.

Two further layers of detail turn the DMM into a key tool in shaping each customer’s digital transformation, guided by the customer’s own priorities:

- A set of capabilities for each pillar and a maturity scale of 1 (Laggard) to 4 (Best Practice) for each capability; and
- The approaches to deliver each capability.



More information about the Digital Maturity Model is available from your Microsoft contact upon request.

CASE STUDY 1

Medifi

After Freddy Gonzalez experienced trouble in connecting with his US-based doctor while in Manila, he decided to co-found Medifi in 2014. The Manila-based start-up delivers remote healthcare solutions by providing a cloud-enabled platform that connects patients to medical professionals regardless of location. Patients have access to video consultations, messaging, medical imaging, and a personal health profile that allows medical consultations from the convenience of their own homes or offices.

One of the most pressing healthcare challenges in the Philippines is the shortage of doctors to meet the health needs of Filipinos. The Philippines has a ratio of one doctor for about every 33,000 patients, while, for example, Cuba has a ratio of one doctor for every 1,075 patients. Many healthcare centers are also not within patients' geographical reach. Taking hour-long queue at local clinics for often short consultations can be a daunting experience for patients, further emphasizing the need for a solution to make remote consultation possible.

Medifi currently has dozens of doctors from both the Philippines and the United States using its service and expects to bring more on board to help cater to the growing demand. While the service is not meant to replace face-to-face visits, Medifi has already made pre-visit evaluation and post-treatment follow-ups a lot more convenient, thereby bringing down barriers to healthcare access. It will soon further integrate with commercially available biometric devices delivering a more accurate and comprehensive diagnostic experience online.

The startup has also been successfully integrating personal health technologies and devices, like Microsoft Health and the Microsoft Band app, that collect data from patients' vital signs automatically and accurately and provide actionable insights for people to improve overall health.

> "Utilizing digital technologies and the internet, we are on a mission to improve Filipinos' access to healthcare. Around 70 per cent of clinical visits are avoidable, and these place a heavy but unnecessary strain on the healthcare system."

Freddy Gonzalez, Medifi Co-founder and CEO

PILLAR 3

Partnering with the right cloud services provider

Summary

Although there are no specific due diligence requirements applicable to the adoption of cloud services in healthcare, the healthcare institution should still carry out appropriate due diligence to ensure that the cloud services provider can meet the applicable operational, security, risk management and compliance requirements. To ensure that they are getting a compliant solution, the healthcare institution should develop a set of due diligence and selection criteria mapped against the key regulatory requirements.

Recommendations

Whilst a summary of all applicable compliance obligations is outside the scope of this paper, the table below summarises what we believe are the key cloud services provider selection criteria, based on the underlying regulations and guidance and our conversations with customers. Healthcare institutions may wish to refer to these criteria as part of their cloud procurement.

Confidentiality and Security	Given the sensitive nature of information that is held by healthcare institutions, it goes without saying that the chosen cloud solution needs to be secure. A healthcare institution must ensure that the cloud services provider has a sufficient security system in place to protect against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing, taking into account the nature of the personal data to be protected, the risks involved, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Compliance with international security standards such as ISO/IEC 27001 and ISO/IEC 27018 has become an industry standard tool, in the Philippines and around the world, for cloud customers to verify that their cloud services provider meets the necessary confidentiality and security requirements. A healthcare institution should check whether the cloud services provider notifies it of any data breach incidents and what steps it takes to resolve those incidents. This is because the NPC requires a healthcare institution to notify it of data breaches and may institute investigations on matters affecting personal data. A healthcare institution should also check whether the cloud services provider uses encryption. Not only is encryption an important tool in protecting data, it is also an expected requirement as part of any approval process for a government agency to use off-premises solutions. See "Is regulatory approval or registration required?" under Pillar 1, above, for details of the approval requirement.

Monitoring and Assessment

It is prudent for the healthcare institution to ensure that it can periodically monitor, evaluate and control the cloud services provider, including by obtaining regular reporting and information.

There is no requirement for on-site audit or inspection of the cloud services provider but it is recommended that a healthcare institution ensures its cloud services provider is subject to independent third party assessment. Where a cloud services provider is regularly assessed by independent third parties and shares the results with its customers, the healthcare institution can be confident that the cloud services provider can meet the necessary regulatory requirements on an ongoing basis.

Data Location and Transparency

As outlined in Pillar 1, above, a healthcare institution can store data outside of the Philippines as long as the applicable conditions are met. To help it determine the requirements that apply and whether the applicable conditions are met, a healthcare institution will want to check whether the cloud services provider is transparent as to its approach to data location.

Resilience and Business Continuity

A healthcare institution will want to establish a credible internal process to manage the risks associated with any services arrangements which may include business continuity and disaster recovery plans. A healthcare institution will also want to ensure that services arrangements do not create a risk that its operation and management could be interrupted for a material length of time.

Cloud Services Provider Reputation and Competence

A healthcare institution will want to carefully consider the cloud services provider's track record in the healthcare industry, not just in the Philippines but also around the world. This is not a specific regulatory requirement but is important for providing valuable insight into the cloud services provider's capabilities, track record and global standing.

Conditions on Subcontracting

There is little value in finding the right cloud services provider if that cloud services provider will simply subcontract all of its obligations to a third party that may not meet the necessary requirements. A healthcare institution must ensure that proper safeguards are in place to ensure the confidentiality of the personal data processed, prevent its use for unauthorized purposes, and comply with regulations on personal data processing.
A healthcare institution should therefore:

i. request a list of subcontractors and ensure there is a mechanism for the cloud service provider to notify it of any updates to the list;

ii. ensure that that the cloud service provider takes overall responsibility for compliance; and

iii. ensure that the cloud service provider only uses subcontractors that are subject to controls that are equivalent to those applied by the cloud service provider itself.

Ability to Terminate	Whilst cloud services are often looked at as a long-term solution, it is important that a healthcare institution ensures there are measures are in place in the cloud contract with its cloud services provider to address the healthcare institution's rights to terminate the cloud services as circumstances change or for performance issues.
Conditions on Termination	The DPA requires that data is not held for any longer than is necessary. A healthcare institution should therefore make sure that, on termination or expiry of the cloud contract, the cloud services provider returns its data and then permanently deletes the data from its system.

How Microsoft helps

Microsoft understands that, wherever you are on your journey to the cloud, it is vital to work with a service provider that you can trust. Not all clouds are created equal — it is crucial to check the facts and know what you are getting.

Microsoft confirms its ability to meet all of the criteria specified above. Our understanding of the healthcare industry, based on experience of working closely with healthcare institutions and industry stakeholders over a number of years, is market-leading. Microsoft has over 40 years of IT experience, including decades as a cloud services provider running some of the largest online services in the world, and a proven track-record of successful rollouts for healthcare institutions in the Philippines and globally. We are proud of leading the way when it comes to offering cloud services that can help healthcare institutions maintain compliance with applicable laws, regulations, and key international standards.

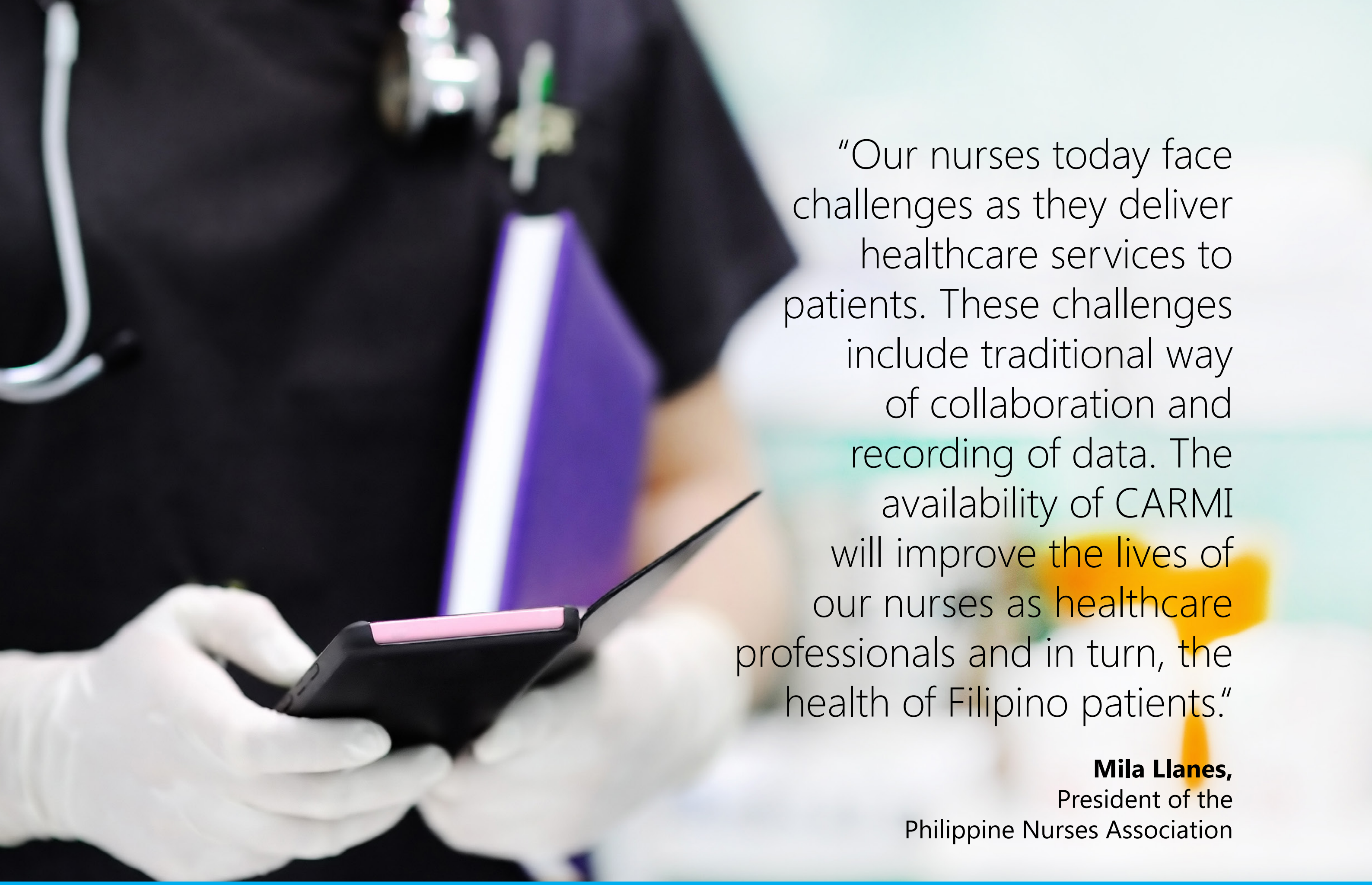
We build our cloud services based on the core principle of trust. We are committed to ensuring that your data stays secure, that it stays private and under your control, and that if you use the Microsoft cloud, you stay compliant, even as regulations and standards evolve. We are also committed to being transparent about our security, privacy, and compliance practices. We make sure you know how your data is stored, accessed, and secured, and that you can independently verify this.

We are also committed to reliability and choice. That is, our software and services are robust to ensure you can access your data and services when you need to, and we give you the final say in decisions that impact compliance.

Microsoft invests heavily in compliance to meet multiple regulatory standards. We design and build services using a common set of controls, making it easier to achieve compliance across a range of regulations, even as they evolve. Our approach to security compliance includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis. We've been able to maintain and expand a rich set of third-party certifications and attestations that you can point to in order to demonstrate compliance readiness to your customers, auditors, and regulators. These include ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2. As part of our commitment to transparency, we share third-party verification results with our customers.

Payer	Provider	Public Health & Social Services	Life Sciences & Pharmaceuticals	Global
ISO 27001/ ISO 27018 EU Model Clause HIPAA BAA FedRAMP	ISO 27001/ ISO 27018 EU Model Clause HIPAA BAA	ISO 27001/ ISO 27018 EU Model Clause HIPAA BAA FedRAMP	ISO 27001/ ISO 27018 EU Model Clause HIPAA BAA	Australia Gov IRAP/ISM Singapore MTCS UK G-Cloud Article 29 WP Japan CS Gold Mark

You can access more detailed information about the robust confidentiality and security at the core of each Microsoft cloud service in the Microsoft Trust Center at microsoft.com/trust.



"Our nurses today face challenges as they deliver healthcare services to patients. These challenges include traditional way of collaboration and recording of data. The availability of CARMI will improve the lives of our nurses as healthcare professionals and in turn, the health of Filipino patients."

Mila Llanes,
President of the
Philippine Nurses Association

CASE STUDY 2

Care Mobility Initiative (CARMI)

Throughout 2014, Microsoft was in discussions with various Philippine healthcare organizations and hospitals to assess the needs of the sector and evaluate how Microsoft could help the industry meet them. To address the identified challenges, Microsoft and HP launched in 2015 the Care Mobility Initiative (CARMI), a pioneer healthcare mobility app in the Philippines.

The CARMI app aims to tackle some of the main challenges that nurses face in delivering healthcare services to patients, including difficult collaboration and overwork. Due to the amount of paperwork and medical records they need to file after long hours caring for patients, nurses are also prone to sleep deprivation.

The CARMI app empowers nurses with technologies specifically tailored to the Philippines healthcare industry. Integrating Microsoft's Office 365, Skype, Microsoft Dynamics Social Media Listening Tool, Electronic Medical Records, Hospital Information System, and Learning Management System, the solution has allowed many Philippine nurses to be more productive, acquire up-to-date skills, and collaborate as care teams, anytime, anywhere, resulting in better health outcomes for patients.

Since its launch, the app – that works on HP devices such as HP Stream 8 and HP Pavillion X2 – has also helped significantly reduce paperwork. This enabled nurses to spend more time caring for the patients, therefore contributing towards better quality of care and greater hospital efficiency.

Through the use of Microsoft Enterprise Mobility Suite and Azure that enabled simplified device management, the app not only contributed to creating a better working environment by reducing nurse fatigue but also helped achieve better patient satisfaction.

PILLAR 4

A robust contract

Summary

The healthcare institution will want to verify that assurances made by the cloud services provider in response to selection criteria are backed up by appropriate contractual commitments. The cloud contract should include appropriate terms so that the healthcare institution can satisfy itself of compliance with the underlying regulations.

Recommendations

The following terms are those that Microsoft believes to be important, based on the underlying regulations and our discussions with customers in the Philippines. The healthcare institution will want to put in place a binding cloud contract that, as a minimum, includes these key terms. In practice, the cloud services provider should help by demonstrating how its cloud contract meets these requirements.

General information, rights and obligations	The cloud contract must set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects. The cloud contract must set out the obligations and rights of both the healthcare institution and the cloud services provider.
Data location	The cloud contract must specify the geographic location of the processing under the cloud services arrangement.
Data processing and transfers	The cloud contract should only allow the cloud services provider to process, including transfers to other organizations or countries, personal data upon the documented instructions of the healthcare institution, unless otherwise authorized by law.
Regulatory compliance	The cloud contract must ensure the cloud services comply with the DPA, DPA IRR, other relevant laws, and other issuances of the NPC.
Review, monitoring and control	The cloud contract must ensure the cloud services provider makes available to the healthcare institution all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by the healthcare institution or an independent auditor.
Security and data breach protocols	The cloud contract should contain appropriate commitments from the cloud services provider to ensure that information and data are kept secure. The cloud contract should also address what happens in the event of a data breach incident – including any applicable notification, investigation and mitigation protocols.

Business continuity	As part of the healthcare institution's data security obligations and in the interests of ensuring business continuity and resilience matters are addressed, the cloud contract should provide for a disaster recovery/business continuity plan together with appropriate testing processes.
Confidentiality	The cloud contract must ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data.
Termination and exit	The cloud services provider must, at the election of the healthcare institution, delete or return all personal data to the healthcare institution upon termination of the cloud services, unless otherwise required by law.
Conditions on subcontracting	The cloud services provider should only be permitted to subcontract its obligations under the cloud contract with the prior consent of the healthcare institution. Where subcontracting is permitted, healthcare institutions will want to ensure that the cloud services provider takes responsibility for compliance and ensures that any subcontractors are subject to controls that are equivalent to those applied by the cloud services provider itself.

How Microsoft helps

The contractual terms for Microsoft's cloud services have been developed based on feedback from thousands of cloud customers across the most heavily-regulated industries around the world, including customers in the healthcare industry. Microsoft's expert team will be available throughout the contractual review process to answer any questions you have about how Microsoft's contractual terms for its cloud services provide confidence to cloud customers that they are complying with the applicable regulatory requirements and guidelines.

Putting it into practice

Using Office 365 to drive staff productivity

Many healthcare institutions are looking to improve the productivity and effectiveness of their clinical, operational and managerial staff by moving to Office 365. With a single secure synchronised inbox across devices, powerful collaboration and communication tools, staff can work much more efficiently in teams. For healthcare institutions that have traditionally hosted their data locally at their practice, cloud practice management systems enable much greater opportunity for controlled access such as on mobile, from home or at another practice.

Regulatory considerations

Just as they would for on-premises technology solutions, the healthcare institution must comply with general privacy requirements. These include ensuring that they obtain patient consent to the collection, use or disclosure of their data. The healthcare institution must also ensure that data will be kept secure and confidential and, for this reason, Microsoft gives binding contractual commitments regarding the use, disclosure and security of the information.

The healthcare institution should also consider whether any approval or registration requirements apply, as described in Pillar 1, above.

Steps you should take

1. Understand how your organisation is using on-premises equivalents of Office 365 today.
   Is the solution secure? Does it provide the range of services and features available via Office 365?

2. Consider potential use cases for Office 365.
   What productivity and efficiency improvements could be achieved by using a cloud-based solution?

3. Consider any approval or registration requirements and build those into the project timeframe
   See Pillar 1, above.

4. Talk to Microsoft about its cloud adoption checklist
   Microsoft provides a checklist to map Microsoft's cloud services against the applicable regulatory requirements in the Philippines. This checklist helps healthcare institutions in the Philippines adopt Microsoft cloud services with confidence that they are meeting all applicable regulatory requirements. This is available from your Microsoft contact upon request

Using Azure to unlock data insights that help improve population health

Data-driven diagnostics have the potential to improve patient care, reduce costs, optimize treatments and clinical pathways, and facilitate broad-scale research. The ability to analyse massive amounts of data is vital to the future of healthcare. However, keeping pace with and generating value from increasing volumes of data requires ever-faster computing resources and rapidly increasing storage. These are core cloud capabilities, making cloud services the logical option for healthcare analytics.

Cloud-based analytics bring significant benefits to the healthcare industry. They provide the real-time insights you need to monitor and stratify patients according to risk; deliver more reliable, data-driven diagnostics; identify cost inefficiencies and bottlenecks in care pathways; and detect adverse events or other unexpected substandard patient outcomes. Analytics can also help you delve into the data to manage staff productivity or resource deployment. You can also repurpose data for research into optimisation, or even discovery, of new treatments.

Regulatory considerations

The regulatory obligations for the use of aggregated and de-identified medical data are no different in a cloud-hosted model than in a traditional on-premises model. Where the identity of the individual is not apparent or cannot reasonably and directly be ascertained (including when put together with other information) ("de-identified information"), it is not "personal information" for the purposes of the DPA. If personal, health or other sensitive information is de-identified information, DPA requirements applicable to personal information will not apply.

Microsoft can provide data analytics services as an optional value-add to our cloud services. These use aggregated and de-identified medical data to help your practice or organisation with process improvements, health research and discovery, as well as other applications to drive beneficial health outcomes.

Microsoft is committed to using medical data only for the purposes expressly authorised by the practitioner. Microsoft will not undertake aggregated data analytics unless we have your express permission, on an opt-in basis.

If your organisation chooses to participate in the data analytics services, Microsoft makes binding contractual commitments to your organisation regarding the use of your customer data. For almost all of our cloud services, our commitment is to use your customer data only for the purpose of providing the service and compatible purposes, such as troubleshooting or malware prevention. However, for a limited set of Azure Cognitive Services, Microsoft has broader rights to use, retain, reproduce and create aggregated, anonymised data to improve the services themselves, as well as to provide the Cognitive Services. If your organisation chooses to participate, you are required to obtain each data subject's consent to Microsoft processing the data as set out in the Online Service Terms.

Steps you should take

Your organisation will need to consider whether use of data analytics services is consistent with use limitations that attach to your dataset.

These use limitations will vary depending on:

- Whether the dataset contains personal information; and
- To the extent required by the Philippines law, whether any required consents from patients have been obtained.

An unprecedented opportunity to transform the Philippines' healthcare institutions

Healthcare institutions in the Philippines have an unprecedented opportunity to take advantage of the full spectrum of cloud-driven technologies. Driven by an increasingly supportive "cloud-first" regulatory framework, government-led initiatives like the eHealth Vision, rapidly-improving technical infrastructure and a growing range of compliant solutions to choose from, healthcare institutions are beginning to reap the benefits of cloud computing.

Whether it is operational data analytics to streamline operations and reduce costs; virtual health and telemedicine to better connect patients and care teams; clinical analytics to enable more informed choices at the point of decision; or taking raw data from sequencing machines to produce reports on identified genomic variants, just to name a few use cases, the range of opportunities is broad and growing all the time.

At Microsoft, we believe that cloud technologies will play a crucial role in the future of healthcare in the Philippines, and the expansion of the Philippines' vibrant eHealth sector. We look forward to continuing our role at the forefront of this digital transformation, deploying trusted, responsible and inclusive cloud solutions for the benefit of our healthcare institution customers in the Philippines and their patients.

Glossary

“cloud contract“	means the contract between a healthcare institution and a cloud services provider for the provision of cloud services by the latter to the former, such as an outsourcing services agreement which includes the provision of cloud services.
“cloud services“	means on-demand network access to a shared pool of configurable computing resources.
“DPS“	Means the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.
“health data“	means data that has been processed into a particular form which consists of useful values and meanings to improve knowledge in supporting health development.
“healthcare institution“	means the full spectrum of public and private sector healthcare operations in the Philippines.
“patient“	means a person receiving and/or registered to receive medical treatment from a healthcare institution.
“patient data“	means health data relating to a patient, including the patient's medical history and complaints, the medical practitioner's physical findings, the results of diagnostic tests and procedures and medications and therapeutic procedures.
“personal data“	means any data that relates to an individual, including personally identifying information and personal information associated with or derived from an individual’s use of a healthcare institution’s services.
“personal information controller“	means a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes: (i) natural or juridical persons who perform such functions as instructed by another person or organization; and (ii) natural persons who processes personal data in connection with his or her personal, family, or household affairs.
“personal information processor“	means any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.
“public cloud services“	are cloud services in which the infrastructure is owned and managed by a cloud services provider and is located off-premises from a public institution. Although data and services are protected from unauthorized access, the infrastructure is accessible by different customers of the cloud services provider. Public cloud services are also referred to as a “multi-tenanted solution“ because there are multiple customers who will all have access to the same infrastructure.

“sensitive personal information“	includes, amongst others, information about a person’s health, race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations.
“regulations“	means laws, regulations and regulatory guidelines which govern the use of cloud services by healthcare institutions, including privacy regulations.

Further information

Navigating Your Way To the Cloud: **microsoft.com/en-sg/apac/trustedcloud**

A Cloud for Global Good | Microsoft: **news.microsoft.com/cloudforgood/**

Microsoft in Health: **microsoft.com/health**

Digital Transformation in Health: **healthdigitaltransformation.com**

Trust Center: **microsoft.com/trust**

Service Trust Portal: **aka.ms/trustportal**

Online Services Terms: **microsoft.com/contracts**

Service Level Agreements: **microsoft.com/contracts**

SAFE Handbook: **aka.ms/safehandbook**

Microsoft

This document is not intended to be a comprehensive analysis of all regulations and their requirements, nor is it legal advice; rather it is intended to be a summary and to provide guidance to healthcare institutions in the Philippines on the types of issues they should consider.
The information in this document is accurate as of March- 2017.