Microsoft

A Cloud for Global Good

Navigating your way to the cloud in healthcare

A practical guide for the healthcare industry in New Zealand

Towards a digital future for healthcare in New Zealand

We live in a period of dramatic progress in the quest to improve healthcare services through technology.

New Zealand is already at the forefront of the digital transformation of healthcare on a global scale. The Canterbury Health System is piloting a cloud-based application to allow clinicians to safely share confidential patient information on the go, enabling better integrated care and health outcomes for patients. Wellington-based Volpara Health Technologies is making its revolutionary breast density assessment software available to users globally via the cloud, enabling cancers to be detected earlier. Plunket, the country's largest provider of health support services for children under the age of five, has enabled its healthcare professionals to spend more time working with families by adopting a cloud-based system to manage the more than 60,000 clinical records it creates every year.

These organisations are not alone. Across New Zealand, healthcare institutions[1] 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, this digital transformation 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. New Zealand's experience exemplifies this. The digital transformation of New Zealand's healthcare sector has been complemented by an increasingly transparent and supportive regulatory framework; and the expanded use of digital technologies, including the cloud, is now an essential component of healthcare policy in the New Zealand government's Digital Health 2020 plan.

In the past, the pace of cloud adoption in New Zealand's healthcare sector was slower than in other regulated sectors, largely because of concerns about the regulatory environment. These concerns typically focused on barriers to the transfer of data outside of New Zealand and on the ability of cloud services providers to ensure a high level of security and privacy in relation to sensitive information held by healthcare institutions.

Fortunately, that has now changed. Through a series of conversations with healthcare institutions, District Health Boards (DHBs)[2], and other industry stakeholders over a number of years, the Ministry of Health (MOH) has given a green light to the use of accepted cloud services by healthcare institutions. Whilst matters such as data privacy and security remain at the core of the healthcare regulatory environment in New Zealand and must be addressed as part of any technology adoption, there is now widespread acceptance that cloud services can comply (and even enhance the level of compliance) with the necessary regulatory requirements in New Zealand.

The positive outlook for the healthcare sector in New Zealand inspires us. Having partnered with healthcare institutions on many high-profile technology projects in New Zealand, and having

[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 New Zealand, including DHBs, public and private hospitals, surgeries and clinics. The regulations that apply to your institution may differ depending on the nature of your institution – for example, certain rules that apply to public institutions, and specifically District Health Boards, do not apply to private institutions. You should seek advice on this from your legal counsel.

[2] District Health Boards and other government agencies which fall under the mandate of the Government Chief Information Officer (GCIO) have additional requirements including using a DIA IaaS Common Capability Provider and undertaking a risk assessment as per GCIO requirements. GCIO has provided updated guidance and resources for government agencies to adopt and use cloud services. See: https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/

participated for many years in the industry conversations that have led the sector to these exciting crossroads, we have cultivated knowledge and developed practical resources to help healthcare institutions navigate the regulatory landscape for cloud adoption.

This regulatory experience supplements our deep understanding of the business needs of healthcare institutions. In collaboration with McKinsey's healthcare practice leads and subject matter experts, we have created the Digital Maturity Model to enable healthcare customers to focus on the components of a digital transformation that are most likely to have the greatest impact.

> *"There is now widespread acceptance that cloud services can comply (and even enhance the level of compliance) with the necessary regulatory requirements in New Zealand."*

This paper is a further contribution to the digital transformation of New Zealand's healthcare sector. Designed as a practical roadmap, it will help New Zealand's healthcare institutions take full advantage of the transformational benefits of cloud technologies based on a better understanding of the regulatory framework. We also share examples of how cloud technologies are already transforming the way healthcare services are provided.

We hope this paper is useful and look forward to continuing the conversation as we seek to realise our mission of helping New Zealand's healthcare institutions in their journey towards a digital future. We are committed to ensuring that the healthcare institutions in the country 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.

Michael Brick
Legal Counsel, Corporate Affairs Director
Microsoft New Zealand

Barrie Sheers
General Manager
Microsoft New Zealand

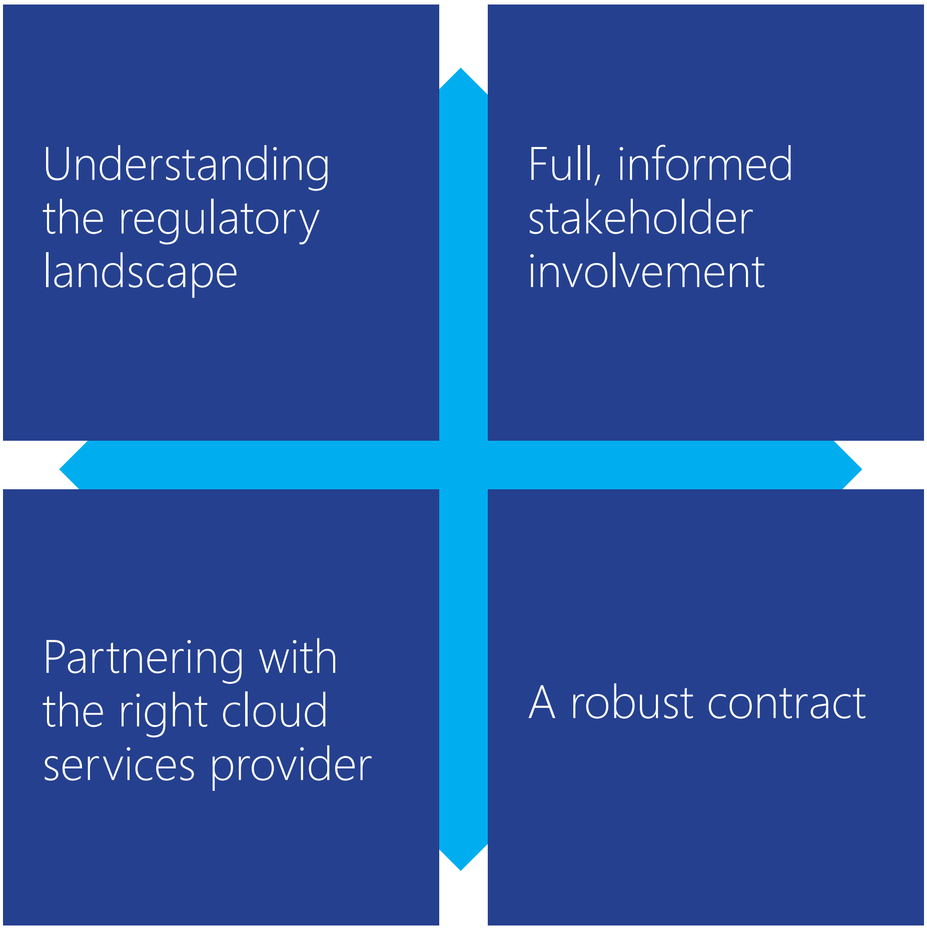
OVERVIEW

The four pillars of a successful cloud adoption

Based on Microsoft's experience of working with healthcare institutions in New Zealand 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 New Zealand 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 New Zealand, 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?	**Ministry of Health (MOH)**. MOH has overall responsibility for the management and development of the New Zealand health and disability system. MOH is also the funder, purchaser and regulator of public health and disability services. **Government Chief Information Officer (GCIO)**. GCIO is the functional leader for government ICT and is responsible for ICT-enabled transformation across government agencies. GCIO has developed the Cloud Computing Risk and Assurance Process, which applies to all State Service agencies and DHBs. GCIO also manages certain Common Capability Contracts. **Office of the Privacy Commissioner (OPC)**. OPC is the primary body responsible for administering the Privacy Act 1993, and issues sector-specific Information Privacy Codes, including the Health Information Privacy Code (HIPC).
What regulations and guidance are relevant?	Key accountability documents that expressly refer to cloud services include: • The "Use of cloud or hosted services for managing health information" advice administered by MOH which DHBs must comply with by virtue of their Crown Funding Agreement (CFA) with MOH and related operational policy framework (OPF); • The Health Information Security Framework (HISF) for the New Zealand health sector, which DHBs must comply with by virtue of their CFA and OPF; • GCIO's[3] "Cloud Computing: Information Security and Privacy Considerations"[4] and resources mentioned in that document –

	including GCIO's "105 questions",[5] which government agencies that fall under GCIO mandate are directed to comply with; • The "Cloud Computing – A guide to making the right choices" (February 2013) guidance issued by OPC, and the "Cloud Computing Checklist for Small Business"; • Health and Disability Services (Safety) Act 2001 (HDSSA) and Service Standards approved under that Act; • Public Health and Disability Act 2000 (PHDA); • Health Information Privacy Code (HIPC); and • The Privacy Act 1993 (which applies to all information about "identifiable individuals").
Are transfers of data outside of New Zealand permitted?	**Yes,** as long as the healthcare institution follows the right process. See "The Regulatory Process: Practical Steps", below, for an overview. However, public sector health agencies may also be required to use common capability contracts for IaaS (i.e. for storage and computing purposes).
If data is stored outside of New Zealand, does it need to be repatriated?	**No.** This was previously a requirement of MOH, however MOH has confirmed that this requirement no longer applies.
Is regulatory approval required?[6]	**No,** if the cloud service has already been accepted by MOH for purposes of storing identifiable personal health information overseas. Microsoft's core cloud services (Azure Core Services, Office 365 Services, Dynamics CRM Online Services) have been accepted by MOH. **Yes,** if the cloud service has not already been accepted by MOH for purposes of storing identifiable personal health information overseas.

3 GCIO has provided updated guidance and resources for government agencies, which apply to DHBs to adopt and use cloud services. See: https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/

4 See: http://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf.

5 To help government agencies undertake their analysis and evaluation of Microsoft enterprise cloud services, Microsoft New Zealand has produced a series of documents showing how its enterprise cloud services address the questions set out in the "Cloud Computing ISPC" by linking them to the standards against which Microsoft cloud services are certified. These certifications are central to how Microsoft assures both public and private sector customers that its cloud services are designed, built, and operated to effectively mitigate privacy and security risks and address data sovereignty concerns. See: https://www.microsoft.com/en-us/trustcenter/compliance/nzcc

6 As of the writing of this paper, we understand that MOH is revising its policy around the use of cloud services for storing identifiable personal health information overseas, with a view to further streamlining and simplifying the process for adoption of cloud services.

The Regulatory Process: Practical Steps

1. Choose an accepted product or service for storing identifiable personal health information overseas. Either choose a product or service accepted by MOH, or apply to MOH for an exemption.[7]

2. If you are a DHB:
   - **A** If you want to use IaaS, you may also be required to procure through the DIA IaaS Common Capability provider.
   - **B** You must undertake a risk assessment as per GCIO requirements (i.e. GCIO 105 questions) – see GCIO Cloud Computing Risk and Assurance process.
   - **C** In respect of Platform-as-a-Service, DHBs will need to apply through the MOH exemption process.

3. If you are a "government agency" and want to use office productivity tools (such as Microsoft Office 365): You will need to conform to GCIO guidelines regarding security.[8] Your cloud services provider should be able to provide guidance on how to achieve conformity. Please ask your Microsoft contact for more information regarding GCIO security guidelines.

4. Satisfy yourself that the product or service has met the requirements of HISF (Cloud Computing and Outsourced Processing).

How Microsoft Helps

Microsoft is pleased to confirm that its core cloud services (Azure, Office 365 and Dynamics) have met MOH's requirements for storage of identifiable personal health information overseas and are accepted.

Close cooperation with MOH, healthcare institutions, and GCIO in relation to a number of successful cloud adoptions in New Zealand has given Microsoft an in-depth understanding of the regulatory framework and process. Issuing this paper is part of Microsoft's commitment to its healthcare sector customers to help them navigate and comply with the regulatory framework as it applies to cloud services. Microsoft's team will be on-hand throughout the process of cloud adoption 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.[9]

[7] As of the writing of this paper, we understand that MOH is revising its policy around the use of cloud services for storing identifiable personal health information overseas, with a view to further streamlining and simplifying the process for adoption of cloud services.

[8] See: https://www.ict.govt.nz/assets/Uploads/Security-Requirements-for-OH-Office-Productivity-Jan-2017.pdf

[9] You can access more information on how Microsoft meets New Zealand specific requirements at www.microsoft.com/en-us/TrustCenter/Compliance/NZCC.

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. A key part of this is a detailed understanding of the proposed technology 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 provide 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 from day one.

The **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 **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 **board** and **senior management** of the healthcare institution 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 technology procurement project requires that all of the 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 de facto deployment model for most organisations.

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 institution should also obtain detailed product and service information from the cloud services provider. Not all cloud services are (or will be) accepted for use by healthcare institutions in New Zealand so 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 assisting with the MOH and GCIO engagement process, as applicable. Our cloud product range spans all of the above cloud service and deployment models and 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.

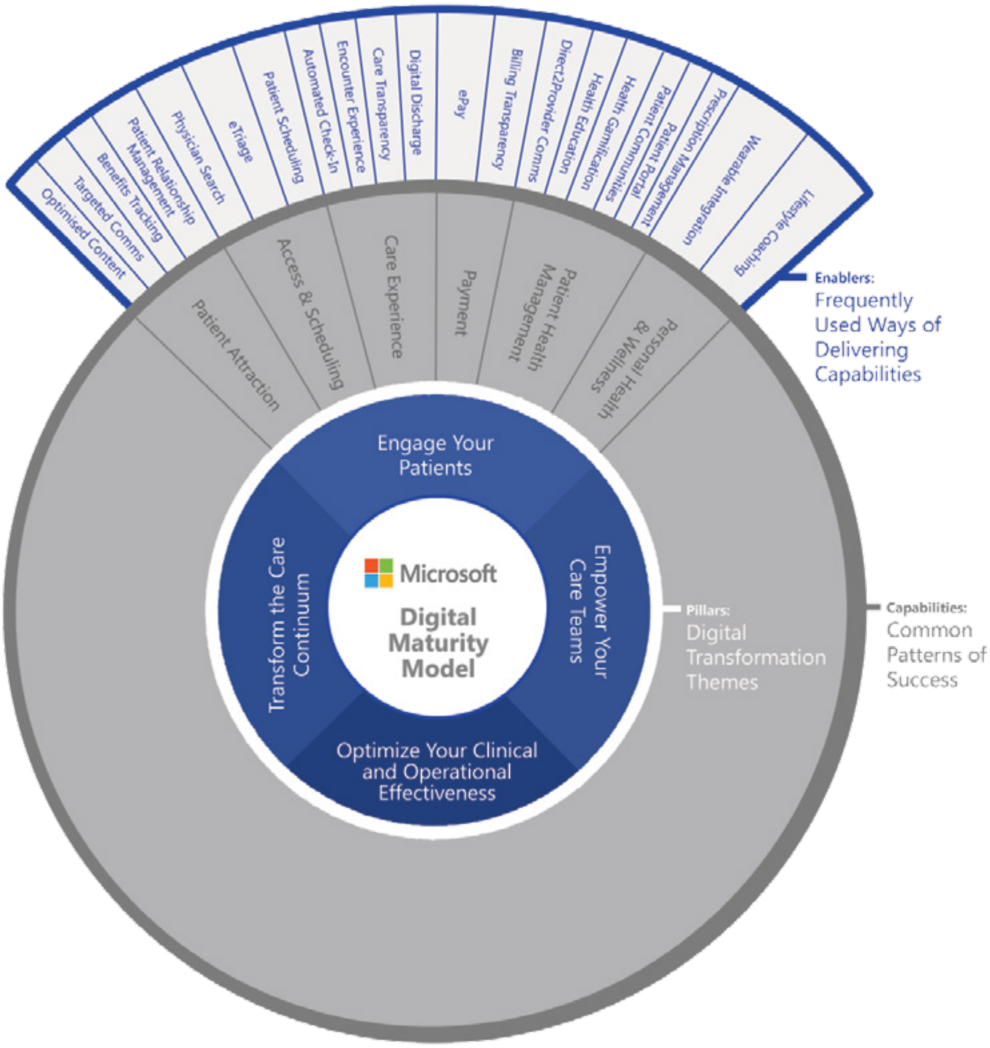
For healthcare institutions seeking end-to-end advice and support in relation to transformative digital projects, we have developed the Digital Maturity Model (DMM). Developed in association with healthcare practice leads and subject matter experts from McKinsey, as well as Microsoft's own subject matter 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.

"It was tough getting the operations and clinical teams over the line which is not surprising. They're the ones that are going to be the most skeptical as they viewed more automation and change as being too uncertain. Once we got them to envision an outcome they believed in, one where they could see the benefits to be reaped, they were in a rush to get there."

Simon Challies
Managing Director
Ryman Healthcare

CASE STUDY 1

Ryman Healthcare

Ryman Healthcare is a leading retirement village operator, operating 30 retirement villages in New Zealand with 6,000 village units and aged care beds. The company is also embarking on expanding its operations into Australia.

Losing their head office in the February 2011 Christchurch earthquake made Ryman Healthcare nervous about how they stored information. They realised that it was risky to depend on manual and paper-based documentation, especially when managing patient care information. They also wanted to mitigate risks of documentation errors.

Its solution was to digitise its business processes so they could be captured and analysed more easily, cutting down any possible errors in its interactions with the older people under its care. This single digital project provided the fuel for Ryman Healthcare to use data in transforming staff productivity and ultimately, enhancing customer experiences.

"The status quo was not acceptable," said Simon Challies, Managing Director of Ryman Healthcare. The company now aims to have 95 per cent of processes digitised. Up until two years ago, 95 per cent of them were carried out with pen and paper.

Ryman Healthcare is working to develop myRyman, a tablet-based nursing app running on Microsoft Surface devices and Azure cloud services. The app will help handle the staff roster, let staff communicate with one another and check which residents they are expected to see on the day. When it is complete, myRyman will also provide transparency to residents, giving them an opportunity to understand how Ryman Healthcare staff are working around the clock to provide the best patient care.

Although the initial aim was to solve one business problem – mitigating risks – business digitisation efforts have since changed the way Ryman Healthcare does business as well.

Digitising its business processes and interactions with seniors in the retirement villages has enabled Ryman Healthcare to generate useful insights and analyses on Microsoft Azure, therefore forming the foundation for the company's subsequent business transformation.

Today, the core of what Ryman Healthcare is driving through their efforts to further digitise their business is to get better insights to enable caregivers, residents, doctors and nurses to maximise the time they spend on patient care.

PILLAR 3

Partnering with the right cloud services provider

Summary

New Zealand's healthcare regulation and guidance recognise that not all cloud services are created equal. Only a limited number of cloud services providers can meet the stringent privacy and security standards required by regulation in New Zealand. Accordingly, healthcare institutions need to carry out appropriate due diligence. For example, MOH and GCIO require DHBs to undertake due diligence of the cloud services provider, whether the data is domiciled locally or not, which includes following GCIO's "Cloud Computing: Information Security and Privacy Considerations". Due diligence is also required as part of healthcare institutions' obligations to take reasonable steps to keep health information secure under the HIPC. 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 Standards	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. The due diligence process should focus on ensuring that the cloud services provider has measures in place to ensure compliance with the required confidentiality and security standards in New Zealand. These include: • Requirements under the Privacy Act and HIPC not to disclose personal information or health information except in compliance with the 12 information privacy principles set out in those documents, and to use security safeguards that are "reasonable in the circumstances" to guard against loss, access use, modification, or unauthorised disclosure, or other misuse of such information; • Requirements in relation to privacy and records under the relevant service standards and the HDSSA; and • Rules under the general laws regarding breach of confidence and ethical duties of patient confidentiality. Compliance with international security standards such as ISO/IEC 27001 and ISO/IEC 27018 has become an industry standard in New Zealand and around the world.

Review, Monitoring and Control

The healthcare institution will want to ensure that the cloud services provider has in place appropriate measures to enable the healthcare institution to review, monitor and control the cloud services. This is both good operational practice and a specific requirement under certain underlying regulations. For example, there is an express obligation for DHBs to monitor the performance of service agreements under section 25 of the PHDA and other public entities are likely to be under similar monitoring obligations from various sources.

Data Location and Transparency[10]

The transfer of data outside of New Zealand is permitted if the cloud service is accepted by MOH for purposes of storing identifiable personal health information overseas. Healthcare institutions should ask and assure themselves where their data will be stored.

Limits on Data Use

Cloud services providers should not use the healthcare institution's data for any purpose other than that which is necessary to provide the cloud service. The cloud services provider should therefore commit not to use it for any secondary purpose, such as advertising. This limitation on data use is a specific requirement under the HIPC (agencies must only use health information for the same purpose for which they obtained that information) and under the more general obligations of the Privacy Act.

Data Segregation

Whilst there are no specific requirements concerning segregation of data under the regulations, this is an important consideration when ensuring confidentiality and security, since if the data of one cloud customer is accessible by another cloud customer, the confidentiality and security of that data would be compromised. There are no requirements for physical separation of data and, through its acceptance of various public cloud services (including Microsoft cloud services), MOH has confirmed that logical separation of data is sufficient to meet the necessary requirements.

Resilience and Business Continuity

The resilience of healthcare institutions' systems is of utmost importance given the nature of their operations. These healthcare institutions therefore need to satisfy themselves that their use of third party services does not threaten the continuity of their operations. DHBs are subject to relatively detailed requirements, including having a health emergency plan, and including certain commitments in supply agreements for goods and services relating to compliance with the DHB's health emergency plan. In addition, some business continuity or resilience obligations are likely to be implied into all health institutions' obligations under the Privacy Act and HIPC (including the obligation to subject personal information and health information to reasonable security safeguards).

[10] As of the writing of this paper, we understand that MOH is revising its policy around the use of cloud services for storing identifiable personal health information overseas, with a view to further streamlining and simplifying the process for adoption of cloud services.

Cloud Services Provider Reputation and Competence	By accepting the cloud services of only a limited number of cloud services providers for purposes of storing identifiable personal health information overseas, MOH has emphasised the importance of finding the right cloud services provider partner. Healthcare institutions will want to carefully consider the cloud services provider's track record in the healthcare sector, not just in New Zealand but also around the world. This is important not only for complying with the necessary due diligence requirements but also for providing valuable insight into the cloud services provider's global dealings and standing.
Conditions on Subcontracting	Whilst there are no specific requirements on subcontracting imposed by MOH or other applicable regulators, 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. Seeking a comprehensive list of subcontractors will often be impractical (not least since those subcontractors may change for operational reasons) and is not required by regulation or guidance. However, healthcare institutions will want to ensure that the cloud services provider takes primary responsibility for compliance from a contractual perspective and only uses subcontractors that are subject to controls that are equivalent to those applied by the cloud services provider itself.
Conditions on Termination	Whilst healthcare institutions will often look at cloud services as a long term solution, they should be prepared for a scenario where the cloud services are terminated. Whilst there are no specific regulations or guidelines concerning the termination of cloud services, in practice the HIPC and Privacy Act will mean that the institution will want the cloud services provider to commit that information will be securely returned to the institution or deleted.[12]

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 sector, based on our experience of working closely with MOH, GCIO, 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 has a proven track-record of successful cloud rollouts for healthcare institutions in New Zealand and globally. We're 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.

[11] As of the writing of this paper, we understand that MOH is revising its policy around the use of cloud services for storing identifiable personal health information overseas, with a view to further streamlining and simplifying the process for adoption of cloud services.

[12] Unless backups are kept separately, note that destruction may not always be an option for a healthcare institution, as there are obligations to maintain health records for certain minimum periods under the Health (Retention of Health Information) Regulations 1996 (issued under the Health Act) and the Public Records Act 2005.

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. And we are committed to beingtransparent 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 270018 EU Model Clause HIPAA BAA FedRAMP	**ISO 27001/ ISO 270018 EU Model Clause HIPAA BAA**	**ISO 27001/ ISO 270018 EU Model Clause HIPAA BAA FedRAMP**	**ISO 27001/ ISO 270018 EU Model Clause HIPAA BAA**	**Australia Gov Singapore MTCS UK G-Cloud Article 29 WP IRAP/ISM**

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.

CASE STUDY 2

Stand Children's Services

Stand Children's Services provides a wide array of services for children and families who have been exposed to many adverse experiences in their lives such as poverty, violence and trauma. From prevention and intervention, to enrichment and residential treatment, all of Stand's services focus on restoring hope, trust and confidence while building the skills and resilience to live safe and fulfilling lives.

Dr. Fiona Inkpen, Chief Executive of Stand Children's Services (Stand) strongly believes that no two children are alike. Guided by this belief, in 2004, Stand took the bold step of adopting an individualised approach for the high-risk children and families that they serve. However, the 300-strong organisation needed to adapt more swiftly to the needs of each child. Better data management was critical.

As with most non-profit organisations, the process of data collection and analysis had typically only served the purpose of reporting on contracts with government. However, this data collection process provided little ability to improve outcomes. Collated at specific times in the year, the data tended to offer little actionable insight on the factors that drove or hindered performance. Important information such as outliers or high-risk situations were being identified on hindsight, making it challenging for preventive measures to be taken in a timely way.

While traditionally, sophisticated data management and analysis tools have been outside the financial reach of non-profit organisations such as Stand, cloud technology now presents an affordable and quick entry point for many to begin employing data and analytics to improve outcomes and be accountable for results.

In 2016, Stand partnered with Microsoft Gold Data Analytics Partner, Stellar Consulting Group, to launch a cloud-based data and analytics application tailored for social services. Utilising Microsoft's Azure platform and Cortana Intelligence Suite of cloud-based services, Stellar developed a fully

"Non-profit organisations like Stand Children's Services hold rich, untapped datasets that are vital for measuring and improving community outcomes. Unfortunately, a scarcity of resources in this sector means most lack the capacity to derive value from data. Microsoft's cloud technologies now give us the ability to unleash the power of data and analytics quicker, cheaper, more securely and more reliably than ever before for SMBs. I believe this is a true game-changer for public sector productivity and collaboration."

Travis Barker
Consulting Partner
Stellar Consulting Group

"I know what's going on in the organisation at a level I never had previously. I can demonstrate to our funders that we are evidence informed, accountable, risk aware and outcomes focused. This cloud-based solution has allowed us to focus on doing the right things, rather than just doing things right."

Dr. Fiona Inkpen
Chief Executive Officer
Stand Children's Services

featured analytic solution in just six weeks – providing Stand with a level of organisational awareness and insight which had previously been difficult to attain.

This new level of insight is enabling Stand to transform its specialised care model from one that relied heavily on anecdotal disparate knowledge to a dynamic and evidence-informed suite of services. Practitioners now have access to new data daily, to guide interventions at the level of the individual child and family. Clinical leaders also have better oversight, with real-time monitoring and analysis of performance across the entire organisation.

Specifically, the cloud-based data and analytics application is strengthening Stand's social impact by:

- **Mitigating risk through better visibility:** The ability to identify and intervene quickly to complex needs and critical events can prevent an escalation that might have serious implications for a child's safety and wellbeing. Through the application, Stand's practitioners can monitor and assess a child and family's safety and wellbeing. They can also benchmark results across the population Stand serves by age, gender, ethnicity, service type and region. Outliers in a child's behavior that constitute risk can be quickly identified and managed, enhancing the child's safety and development.

- **Improving impact through actionable insights:** With data analytics tools, Stand's staff can now get immediate actionable insight from their data – informing them on what they should be doing rather than what they have done. From the collective data provided by practitioners, Stand's leadership can also identify new trends and determine the appropriate resources, partners and staff training needed to address them. This will enable Stand to deliver a higher standard of care in the long term.

Across New Zealand, the Government spends an estimated lifetime expenditure of $6.5 billion (NZD) on the country's 10,000 most vulnerable people. Despite this significant investment, data shows that financial and social challenges persist for this community. Like Stand, many other social service organisations need to be able to effectively identify the areas of greatest need among their clients and re-allocate expenditure to interventions that will have the greatest impact.

PILLAR 4

A robust contract

Summary

Whilst there are no prescriptive regulatory requirements when it comes to the terms that must be included in the cloud contract, there are various terms that healthcare institutions will want to ensure are addressed in order to satisfy themselves of compliance with the underlying regulations.

Recommendations

The required terms will vary depending on the healthcare institution in question but the following terms are those that Microsoft believes to be important, based on the underlying regulations and our discussions with customers. Healthcare institutions 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 their cloud contract meets these requirements.

Privacy and Data Protection	The contract will need to contain appropriate requirements to enable the healthcare institution to meet its own primary obligations (e.g. ensure that all health information and personal information is dealt with in accordance with applicable privacy and data protection laws).
Security	The HISF requires DHBs to ensure security controls are built into contractual arrangements for cloud services covering (as a minimum) transmission, storage, processing, data centre infrastructure, encryption and decryption of data, recovery of client information and/or applications by the health organisation, and access to client information by third parties.
Availability	As a matter of good operational practice and to ensure requirements regarding business continuity and resilience are addressed, healthcare institutions will want to ensure that the cloud services provider makes binding commitments as to service availability, with specified remedies in the event of an unscheduled service disruption.
Business Continuity	Again, in the interest of ensuring underlying business continuity requirements are met, the contract should provide for a disaster recovery or business continuity plan together with appropriate testing processes.
Confidentiality	In order to comply with patient confidentiality obligations, healthcare institutions will want to ensure that the cloud services provider makes binding commitments regarding the confidentiality of information stored in the cloud service.

Termination and Exit	Whilst there are no specific regulations or guidance concerning the termination and exit provisions that must be included in a cloud contract, in practice the HIPC and Privacy Act will mean that the institution will want the cloud services provider to commit that information will be securely returned to the institution or deleted, as described in Pillar 3, above.

How Microsoft helps

Microsoft understands that commitments made during the due diligence and supplier assessment stages are worth little unless backed up by binding contractual commitments. 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 sector. 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

Scenario 1:
Using Azure to host and share clinical information systems with a patient care team or referral network

Healthcare is collaborative by nature, with clinical teams and specialists playing a shared role in diagnosis, treatment and care. As a result, many organisations are seeking to simplify collaboration across different organisations and clinicians that may be contributing to a particular patient's care.

Regulatory considerations

Azure core services have been accepted by MOH for storage of identifiable personal health information overseas. Healthcare institutions should take into consideration the regulatory landscape and other matters described in Pillar 1, above.

The regulatory considerations in providing cross-organisational care in a cloud-hosted environment are essentially the same as those applicable to providing care in any other environment – the principal concern for healthcare institutions is that patient health information is collected only with consent of the patient, the health information is used and disclosed only for the purposes for which it was collected (except in special circumstances), and the health information is protected from unauthorised use, modification, disclosure or loss.

In some circumstances, compliance with these regulatory obligations is easier in the cloud-hosted environment than in the on-premises or hard copy environments. A cloud-hosted document storage system such as those on Microsoft Azure allows centralised access of all relevant documents and files, including logs and records of who accessed them and when, so healthcare institutions can comply with their information security obligations.

Hosting patient records in the cloud also facilitates team care arrangements by allowing different clinicians and healthcare specialists to access a central and, in some cases, a shared patient record so that all relevant information is available to them no matter where they are – even across organisations, if appropriate.

A centralised system will support compliance with the obligation to ensure records are current, as multiple parties will be able to keep patient information up to date, in real time. You will be responsible for ensuring the right people have the appropriate authorities to access, read, and edit such information. You will need to consider the restrictions you will place on the use and disclosure of records – generally this will be through a combination of service control features (such as role-based access controls) and contractual measures between the participants in the central sharesite.

But it's not just about document storage systems, other systems used by healthcare institutions – including practice management systems and systems for processing electronic medical records – can also be delivered as hosted services by installing them as applications on an "as-a-Service" platform or infrastructure like Microsoft Azure. Unlike an on-premises model, in a platform-as-a-service or infrastructure-as-a-service[13] arrangement, the service organisation is responsible for physical and host security, and the practice management software organisation is generally responsible for security at the

[13] Bear in mind that, if you are a DHB and you want to use an IaaS solution, you may be required to procure it through the DIA IaaS Common Capability provider.

application level, so the healthcare institution need only focus on data classification, client-side security, and identity and access management.

Steps you should take

1 Undertake an assessment as to who needs access within your organisation and those that will need appropriate access outside your organisation.

2 Consider whether to impose additional restrictions in relation to patient records and, if so, how you will reinforce those using cloud service features like role-based access controls, your own additional controls, as well as contractual measures with the participants.

3 Decide who within the organisation is responsible for responding to access and correction requests in relation to data stored in the cloud.

4 Follow the practical steps to navigate the regulatory process, as described in Pillar 1.

Scenario 2:
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

Like Azure, Office 365 has been accepted by MOH for storage of identifiable personal health information overseas. Healthcare institutions should likewise take into consideration the regulatory landscape and other matters described in Pillar 1, above.

Just as they would for on-premises technology solutions, healthcare institutions must comply with general privacy requirements. These include ensuring that they obtain patient consent to the collection, use or disclosure of their data. Healthcare institutions 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.

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 Follow the practical steps to navigate the regulatory process, as described in Pillar 1.

An unprecedented opportunity to transform New Zealand’s healthcare services

With a new and supportive regulatory framework in place and a range of compliant solutions available to choose from, healthcare institutions in New Zealand have an unprecedented opportunity to take advantage of the full spectrum of cloud-driven technologies – whether that 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, to name just a few recent use cases. And new opportunities are emerging all the time.

At Microsoft, we believe that these cloud technologies will play a crucial role in the future of healthcare in New Zealand, and the expansion of New Zealand’s vibrant health technology sector locally, regionally and globally. 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 New Zealand and their patients.

Find out more

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

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

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

Microsoft's Response to New Zealand Government Chief Information Officer's 105 Questions: **microsoft.com/en-us/trustcenter/compliance/nzcc**

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 paper 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 New Zealand on the types of issues they should consider.