Microsoft

Navigating your way to the cloud

A guide for Australian healthcare service providers

Contents

Towards a digital future for healthcare in Australia

Australia's healthcare providers (HCPs)[1] are dealing with increasingly complex digital transformation as they use 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. The opportunities that the cloud offers to transform healthcare are far-reaching. Take, for example, high-performance computing power for initiatives like genomic reassembly and analysis, 3D modelled prostheses and the use of advanced analytics to create predictive models to mitigate risks such as unplanned re-admissions and sepsis.

Despite the interest in cloud technologies and growing list of successful cloud deployments, the pace of adoption has been slower in Australia's healthcare sector than in other regulated sectors. This is partly because of concerns about the regulatory environment; specifically, the ability of cloud services providers (CSPs) to ensure a high level of security and privacy compliance in relation to sensitive information held by HCPs.

This document provides helpful guidance on legal and regulatory healthcare compliance and how Microsoft cloud services help you meet your key requirements. It also looks at cloud usage in the context of common healthcare scenarios and takes you through important considerations and next steps to help you address your risk and responsibility issues in the Microsoft cloud.

We are confident that our comprehensive control environment and contractual commitments provide the right framework for regulated HCPs. And we welcome the opportunity to work with you to explore how patient records and other workloads can be moved to Microsoft cloud services in a manner that is consistent with your compliance needs.

We trust you find this paper useful, and we look forward to continuing the cloud conversation with you.

Dr Nic Woods
Health Industry Executive
Microsoft Australia

Tom Daemen
Director, Corporate, External, and Legal Affairs
Microsoft Australia

1. In this paper, we use the term "healthcare provider/HCP" broadly to refer to the full spectrum of public and private sector healthcare operations in Australia, including public and private hospitals, health insurance providers, aged care institutions, surgeries and clinics.

Common cloud misconceptions

The most common myth is that HCPs are prevented by legislation from moving sensitive health information to the cloud. In fact, there is no blanket regulatory impediment to hosting patient records or other health information in the cloud.

When undertaking due diligence, many of our customers have found that Microsoft's public cloud services offer an increased level of operational security, risk management and compliance relative to a private or hosted cloud, for both sensitive information such as patient records, and non-sensitive information.

The following table provides an overview of common cloud misconceptions. To understand how Microsoft helps healthcare customers meet particular compliance obligations in more detail, see pages 7-10.

My organisation can't move to the cloud because it is illegal, unsafe or a breach of a duty of care to our patients	There is no blanket regulatory impediment to hosting health information in the cloud. Generalisations about the relative risk exposure of cloud services seldom withstand scrutiny. • You should compare the relative risk of maintaining your current system with the proposed cloud service to assess whether Microsoft's cloud allows you to meet your duty of care requirements. • Typically, when our customers conduct a relative risk assessment, they find their existing arrangements have not kept pace with evolving compliance requirements. They also find that they are more easily able to meet their compliance obligations by moving to the Microsoft cloud due to its superior level of operational security, risk management and compliance characteristics.
My organisation can only use a technology service that is specific to HCPs	There is no regulatory impediment to storing health information on shared infrastructure in a public cloud. • In our view it is more important and relevant to assess the risks of public cloud based on the CSP's ability to meet the necessary legal, ethical and compliance requirements, than to base your decision on the markets in which other users of a cloud service operate. • Microsoft cloud customers include a significant and growing number of HCPs and customers from heavily regulated sectors including financial services and government. In our experience these customers have been able to move to Microsoft cloud services in a compliant manner, regardless of their market sector, because we design our cloud services to facilitate our most highly regulated customers' compliance. • For example, Microsoft employs data isolation controls in Azure, Office 365 and Dynamics 365 to segregate each customer's environment and data. (See the table on page 9 for more details).
My organisation will have more onerous legal compliance obligations in the cloud than on premises	Obligations relating to health information in the cloud are no different to those that apply to health information stored on premises. • Most legislative obligations imposed on HCPs relate to the kind of information they collect about an individual, how they collect and use it, what information they need to provide, and the obligations they have to such individuals about that information. • Those obligations don't change (and no additional obligations are imposed) when an HCP moves to the cloud.
All health information must be stored in Australia	There is no blanket law preventing storage of health information offshore – usually offshore storage is permitted if privacy laws in the recipient country match those that apply to you, or if you have the data subject's consent. • Microsoft lets you avoid having to make that risk assessment by committing to store categories of data at rest in the Australian geography. • Many Australian HCPs use cloud services, including Azure, Office 365 and Dynamics 365, that are available from our datacentres in New South Wales and Victoria.
Using a US-based cloud provider like Microsoft exposes my organisation to additional, unacceptable risks	Microsoft contractually commits in its cloud agreements to ensure any third party requests for data must follow due legal process. • The Patriot Act, Electronic Communications Privacy Act and Foreign Intelligence Surveillance Act focus on the investigation of terrorism directed at the US. They do not empower the US Government to conduct 'fishing expeditions'. It is highly unlikely that our HCP customers in Australia would be the subject of a request for data under those Acts. • Microsoft will contest (and has already successfully contested) any attempt by the US Government to compel Microsoft to disclose customer data stored exclusively outside the US. • Microsoft allows the law of the jurisdiction of the datacentre to govern which authorities may have lawful access. • Australian HCPs also benefit from specific contractual commitments to store categories of data at rest in our Australian datacentres. • Microsoft does not build hidden 'back doors' into our cloud services, nor do we provide any government with encryption keys or direct or unfettered access to customer data.
My organisation will have no control over operational oversight or business continuity in the event of a disruption	Real-time and historical information about service performance is available at any time via the administration portal or dashboard of the relevant Microsoft cloud service. • Our cloud services are engineered to be highly resilient. In the unlikely event of a sustained service disruption, you have control of your data, and there are no legal impediments to prevent you ceasing to use the Microsoft cloud service and transitioning back to on-premises installations using established pathways. • You can retrieve a copy of all your customer data at any time and for any reason without requiring Microsoft's assistance.
The My Health Records legislation makes it more difficult to move health information to the cloud	The purpose of the My Health Records Act 2012 (Cth) is to set up and govern a system with a central repository for health records uploaded by HCPs who participate in the My Health Records System. • Any obligations imposed on an HCP under that legislation are unaffected by how that provider itself manages the data it collects, and do not apply to data that the HCP generates independently of the My Health Record System.

Compliance considerations for Australian HCPs

There are no laws or regulations prohibiting the use of cloud services in the Australian healthcare sector. Commonwealth and State Governments are embracing e-health services in general.

Separating public and private obligations

The Australian healthcare sector comprises both public and private HCPs.

There are a number of different and overlapping systems created under Commonwealth law that relate to privacy and health information. The only general obligations that apply to entities handling health information (regardless of their particular relationship with the individual to whom the health information relates) are set out in the Privacy Act 1988 (Cth) (Privacy Act).

Programs such as My Health Records and the Individual Health Identifiers enable HCPs to access patient data with other HCPs. The obligations imposed under the My Health Records Act 2012 (Cth) or the Healthcare Identifiers Act 2010 (Cth), for example, apply only to entities to the extent that they actively participate in the systems to which those Acts relate. Health information generated independently by HCPs is not covered by the obligations under those laws.

The role of the Privacy Act

There are no laws or regulations that relate specifically to cloud services provided to HCPs. However, there are Australian privacy laws that deal with the way in which HCPs collect, use, store and disclose personal information, and these need to be considered when adopting cloud services.

The Privacy Act is the main legislation relevant to data protection in Australia. It sets out the Australian Privacy Principles (APPs), which include obligations in relation to personal information (defined as any information or an opinion about an identified individual, or an individual who is reasonably identifiable) and sensitive information (which includes information about an individual's health).

The role of State and Territory legislation

HCPs may also be subject to State and Territory laws and regulations particular to those jurisdictions that are broadly similar to, and address the same issues as the Commonwealth privacy legislation.

For example, New South Wales, Victoria and the Australian Capital Territory have specific health privacy legislation that covers HCPs in public and private sectors. This means that private HCPs operating in these States must comply with both Commonwealth and State or Territory privacy legislation when handling health information.

Queensland, the Northern Territory and Tasmania have privacy legislation that applies only to public HCPs. Western Australia and South Australia do not have specific privacy legislation. South Australia has administrative directions and codes that apply to the public sector, including HCPs. Public sector HCPs in Western Australia have confidentiality obligations under health legislation.

A list of health privacy laws by jurisdiction is set out in the Appendix on page 22.

How the law applies to CSPs

In general, HCPs must take reasonable steps to ensure that contracted CSPs comply with the APPs or relevant State or Territory privacy principles. HCPs will need to be satisfied that their CSP will protect the relevant information from misuse, interference, loss and unauthorised access.

CSPs dealing with Commonwealth Government agencies must also demonstrate that their service is fit for purpose, provides adequate protection and delivers value for money, according to the Commonwealth Government's National Cloud Computing Strategy.[2]

How Microsoft can help

Microsoft will work with you to ensure you can meet your compliance requirements in our cloud. We can help by providing resources to inform your business case and risk assessments, including mapping tables that illustrate how our cloud services and contractual obligations can help you satisfy each of your privacy and security obligations.

2. https://www.communications.gov.au/sites/g/files/net301/f/National_Cloud_Computing_Strategy.PDF

Your key compliance obligations and how Microsoft can help

The majority of the obligations imposed on HCPs by legislation relate to:

- The collection of health information;
- Keeping health information secure and safe from unauthorised access;
- The use and disclosure of health information by the HCP; and
- The relevant individual's rights to access their health information and correct or annotate it if the individual considers the information to be inaccurate or misleading.

These obligations are relevant to HCPs whether they are using an on-premises solution or a cloud solution.

Not all these obligations will apply to Microsoft, as a CSP. However, we can help you use Microsoft cloud services while still meeting your compliance requirements. It's a shared responsibility.

Collection of health information

Your obligations

The obligations applicable under the relevant Australian legislation broadly require you to:

- Collect health information about individuals only with their consent[3] and in a non-exploitative manner; and
- Make clear (at or around the time of collection) the purposes for which you are collecting the information.

What constitutes health information?

Health information generally means:

- Information or an opinion about:
  - The health or disability of an individual;
  - An individual's expressed wishes about the future provision of health services; or
  - A health service provided, or to be provided, to an individual that is also personal information;
- Other personal information collected to provide, or in providing, a health service;
- Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs, body substances; or
- Genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Non-individualised health information; for example, aggregated data about the healthcare industry that is not attached to identified individuals, will not constitute health information for the purposes of health privacy laws.

Microsoft's role

Microsoft is not the 'collector' of health information. You have control of the relationship with the data subject and so you are responsible for the compliant collection of health information.

3. There are specific legislative exceptions to the consent requirement; for example, in emergency situations.

Keeping health information safe and secure

Your obligations

You must take reasonable steps to protect health information from misuse, interference and loss, and from unauthorised access, modification and disclosure.

How Microsoft can help

Microsoft makes available a variety of resources to help you identify common risk events associated with the use of cloud services.

SAFE handbook[4]

This is a risk event catalogue of approximately 50 of the most commonly assessed risks, to which your organisation can add or subtract, depending on its circumstances. The handbook also provides an explanation of threat modelling, which is a useful technique for a deeper examination of the possible conditions that may result in a risk being realised, and the security mitigations you can implement to reduce the event's probability or impact.

The Office 365 Customer Security Considerations Framework

This maps Office 365 security and compliance features to key risk events or threats. It explains how customers can configure and implement controls to help treat the risks identified.

Detailed isolation control information

We make available detailed information on the controls – both service-side and customer-side – that come with our services. For example, the table to the right details the data isolation controls in Azure, Office 365 and Dynamics 365.

Similar information for the other controls that underpin Microsoft cloud services is available in our mapping documents for frameworks such as ISO/IEC 27001 and the Cloud Security Alliance's Cloud Control Matrix.

In addition to reviewing Microsoft's service-side controls, we recommend that you consider the customer-side controls (such as password management and multi-factor authentication) that you can implement to further treat the risks identified as part of your risk and security assessments.

4. aka.ms/safehandbook

Cloud service	Data isolation controls
Office 365	• All Office 365 services and workloads are built on top of Azure Active Directory and as a result they use the same authorisation and role-based access control (RBAC) model. • All Office 365 requests are mediated through authorisation and access control features in Azure Active Directory. • All Office 365 data sessions are either user-scoped or tenant-scoped, and users can't see outside the tenant scope. • Access to Office 365 objects is controlled via user account permissions that are enforced by Azure Active Directory and operating system access control lists. • The authorisation stack prevents people from accessing data without appropriate credentials. • There is no service code that allows a user from one tenant to execute commands against another tenant.
Azure	• Azure also uses logical isolation to segregate each customer's environment and data. • Data in Azure Storage is controlled with a Storage Access Key (SAK). Shared Access Signature (SAS) tokens can be generated using SAKs to provide more granular, restricted access. • Network controls block customer-to-customer access to Azure services. No internet access is enabled by default.
Dynamics 365	• Dynamics 365 provides customers with logical data isolation through separate SQL databases. • Every Dynamics 365 customer also receives a unique identifier in the service, which restricts access by default to that customer's domain, for customer-to-customer data separation.

Use and disclosure of health information

Your obligations

The relevant privacy legislation outlines the parameters within which you may use or disclose health information that you hold, and sets out conditions that must be met before it can be used or disclosed for any secondary purpose, including sales or marketing.

General use and disclosure requirements

Generally, you must use or disclose health information only for the limited purposes for which it was collected, or a directly related secondary purpose, unless you have the informed consent of the data subject.[5]

The policy motivation of these laws is not to prohibit consensual arrangements between individuals and service providers, but to prevent exploitation arising from free rein over personal information, including health information.

When health information is stored within, or used via, a Microsoft online service you remain responsible for ensuring your use and disclosure of it is consistent with relevant legislation.

Use vs disclosure

The Australian Information Commissioner (AIC) categorises cloud computing as a use of personal information (including health information) by the entity obtaining cloud computing services, and not a disclosure to the CSP, provided that:[6]

1. **The CSP is contractually bound to handle that information only for the limited purpose of performing the services of storing and ensuring the entity may access the personal information.**

How Microsoft helps you comply: We make a contractual commitment to use data stored in Microsoft's cloud only for the purpose of providing the online services, including purposes compatible with providing those services (such as trouble shooting).[7]

2. **The contract requires any subcontractors to agree to the same obligations as set out in 1, above.**

How Microsoft helps you comply: We take contractual responsibility for all acts and omissions of our contractors, and up-to-date subcontractor lists are published on the Trust Center website. Microsoft makes a contractual commitment that subcontractors will be permitted to obtain customer data only to deliver the services Microsoft has retained them to provide and will be prohibited from using customer data for any other purpose.[8]

3. **The contract gives the HCP effective control of how the information is handled by the CSP.**

How Microsoft helps you comply: Our cloud customers retain all rights in, and effective control of, their data; customers can extract, verify, amend or delete their data at any time, and we provide tools, such as Lockbox, for customers to limit Microsoft's access to more sensitive data.

Location

An HCP is generally permitted to disclose personal information to a third party outside of Australia (or, in the case of public sector HCPs in NSW, Vic, Tas, WA[9] and NT, outside of the relevant State or Territory) if any of the following requirements are met:

- The destination jurisdiction has at least substantially similar legal protection of privacy as Australia (or the relevant State or Territory);
- The patient has provided express consent; or
- The recipient agrees to be bound by Australian privacy laws (or State or Territory laws) in respect of that information.

How Microsoft can help

In addition to our commitments set out in the 'Use vs disclosure' section above, Microsoft makes contractual commitments:

- To comply with all laws applicable to our delivery of our online services (which includes the Privacy Act);
- Not to use or disclose customer data to any third party without our customer's instruction or a lawful government access request;
- Not to mine data for advertising or any other secondary purpose, unless you specifically request by opting in to Azure Cognitive Services.[10] This is a key feature of the ISO 27018 code of practice against which Microsoft is audited annually.

Microsoft's cloud services, including Azure, Office 365 and Dynamics 365, are available from our Australian datacentres. We make specific contractual commitments to store categories of data at rest in the Australian geography in the Online Services Terms.[11]

Your obligations to individuals

With respect to any health information you hold about an individual, you must:

- Take reasonable steps to ensure the accuracy of that health information;
- Respond to a request by that individual to provide the health information you hold about them; and
- Update inaccurate health information if asked.

How Microsoft can help

Microsoft customers retain all rights in, and effective control over, all information they upload into our online services. Accordingly, you are always able to comply with the obligations above when using Microsoft's online services.

5. In WA, public HCPs who don't have patient consent to use or disclose health information for directly related secondary purposes may require approval from the WA Health Human Research Ethics Committee. We can help WA customers assess whether that's necessary.
6. Paragraph B.144 Office of the Australian Information Commissioner Australian Privacy Principal Guidelines, https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts.
7. See the General Privacy and Security Terms section of the Online Services Terms, available at https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx.
8. See the General Privacy and Security Terms section of the Online Services Terms, available at https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx.
9. In WA, public HCPs are required to have an agreement with CSPs to mitigate the risks associated with information use and disclosure.
10. For more information see the Cognitive Services section of the Online Services Terms: https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx.
11. Available at https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx.

Healthcare compliance scenarios

Using Office 365 to drive staff productivity

Many HCPs 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, and powerful collaboration and communication tools, staff can work much more efficiently in teams.

The opportunities for HCPs and their staff to improve productivity with the use of cloud-hosted services are broader than the storage and processing of health information. Products like Office 365 provide the productivity benefits of the cloud in relation to administrative and communication tasks that do not necessarily involve any patient health information, and therefore are not subject to the more stringent regulatory obligations that apply to patients' sensitive information.

There are certainly opportunities for cloud-driven productivity gains in handling health information. A Forrester study we commissioned in 2015 found that, on average, HCPs would benefit from a 212% return on investment, and 375% internal rate of return, within three years by adopting Microsoft Office 365.[12]

For HCPs that have traditionally hosted their data locally, cloud practice management systems enable much greater opportunity for controlled remote access such as via mobile device, from home or across multiple practices or clinics.

Regulatory considerations

For non-health information, there is no difference from a regulatory perspective whether an HCP chooses an on-premises solution or a cloud solution.

In addition, HCPs have no additional regulatory obligations in relation to health information being stored and accessed in the cloud than they would collecting, using and disclosing health information of their patients generally. Organisations must obtain patient consent to the collection, use or disclosure of their health information in accordance with the Australian Privacy Principles, and the HCP must protect that information against misuse or unauthorised access, modification or disclosure – just as they would for any other personal information.

Microsoft understands HCPs' obligations to their patients, and gives binding contractual commitments regarding the use, disclosure and security of the sensitive information HCPs put into the cloud. For example, Office 365 complies with ISO 27001, the ISO 27002 Code of Practice, and the ISO 270018 Code of Practice standards. Microsoft regularly engages external independent auditors to monitor our compliance, and those auditors produce reports under the audit standards known as SSAE 16 SOC 1 Type II, and SSAE 16 SOC 2 Type II. Microsoft makes those reports available to customers through the Service Trust Portal.[13]

We know that HCPs may want or need the flexibility to bring their activities back in-house. Microsoft cloud services are designed to ensure that you can retrieve a copy of your customer data at any time and for any reason without requiring Microsoft's assistance. Customer data stored within Microsoft cloud services is directly portable to on-premises versions of the same products and we make tools available to make this even easier. Our contractual commitments specify that when you leave the service or your subscription expires, we will store your customer data in a limited-function account for 90 days to give you time to export the data or renew your subscription. After the 90-day retention period ends, we will disable your account and delete all customer data within a further 90 days for Azure, Office 365 and Dynamics 365.

Steps you should take

- Understand how your organisation is using on-premises equivalents of Office 365 today. What types of data are implicated? Health information? Or personal information that is not sensitive information?
- Decide which classification of data you are comfortable with in the cloud. Have information management policies in place and educate your staff so they understand and adhere to them.
- Ensure that all information has meta-data tagging, classification markings, or defined keywords included to make discovery and detection easier.
- Consider digital rights management processes. Office 365 can detect customer-defined classifications, markings or keywords within documents and flag that they may be more sensitive than people realise. The data can also be temporarily encrypted, quarantining it to alert administrators to act on it.

12. Forrester Total Economic Impact Study Commissioned by Microsoft (December 2015): The Total Economic Impact of Microsoft Office 365 for Healthcare Organizations. See http://health.csa.com.au/wp-content/uploads/2016/04/TEI_Of_Office_365_For_Healthcare_Industry_Customers.pdf for more details.
13. Service Trust Portal: trustportal.office.com

Using the cloud for clinical and operational systems and advanced computing services

HCPs, in conjunction with clinical solution partners, are developing cloud-delivered applications that meet the current needs of the clinical service and scale responsively to meet future needs. After making a careful comparison, many HCPs find they are better able to meet their security and privacy obligations by hosting their clinical information systems applications in Microsoft's Azure infrastructure service.

Regulatory considerations

HCPs have obligations to ensure that their patients' personal and health information is protected against unauthorised access, misuse or loss. These obligations also require that HCPs establish a system for monitoring unauthorised access to that information. In some cases they may also be required to actively audit any reports or records to ensure that those protective measures are effective.

Security

HCPs that keep health records on their premises (either in hard copy or digitally on a computer server) must pay for physical and digital security to protect those records. Those costs must be borne by each HCP, which makes it much more difficult to scale up as the organisation grows.

A cloud-based digital storage platform like those run on Microsoft Azure solves many of these issues. Such platforms allow for security to be centralised and benefit from scale efficiency, as well as providing built-in redundancy to protect against local risks such as fire or flooding.

Microsoft provides many built-in service capabilities to help you examine and verify access, control, and service operation as part of your regular assurance processes. These include:

- The Service Trust Portal[14] – for deep technical trust and compliance information, including recent audit reports for our services, as well as the ISO Statements of Applicability.
- The Office 365 Management Activity API – for visibility into user, admin, system, and policy actions and events from your Office 365 and Azure Active Directory activity logs.
- The Azure Security Center[15] – for visibility into the security state of your Azure resources and the ability to respond to threats and vulnerabilities.

Customers also have access to the documentation and information available on the Trust Center[16] concerning the location of our primary and back-up datacentres, subcontractor lists, and rules for when Microsoft service administrators have access to customer data.

Use and disclosure

Australian health privacy laws do not prevent the use of cloud-based services by HCPs, and no approvals are required from any regulator prior to an HCP procuring a cloud-based IT service. Provided your cloud service satisfies the criteria set by the AIC for use of personal information (discussed above in the 'Use and disclosure of health information' section of this paper), no special consents from patients are required for an HCP to store health information in the cloud. Microsoft implements best industry practice security measures on all of its online products, including the ability to create access logs and audit trails to verify that the security measures are working. This allows HCPs to ensure that their patients' health and other personal information is adequately protected and helps those HCPs to comply with their information handling obligations.

If you are concerned that, contrary to the AIC's guidance, use of our cloud services will constitute a disclosure of your data, you can still use cloud services to store data, including patient records, provided you notify your patients that you use cloud services and obtain each patient's consent to disclose their data to the CSP.

14. Service Trust Portal: trustportal.office.com
15. Azure Security Center: azure.microsoft.com/en-us/services/security-center
16. Trust Center: microsoft.com/trustcenter

Data sovereignty

There is no general prohibition on HCPs transferring patient health information outside of Australia (or the relevant State or Territory).

However, Microsoft recognises that many HCPs are concerned that offshoring health information creates a perception of less control over that health information or that the health information is exposed to the application of unfamiliar foreign laws. To address these concerns, Microsoft offers contractual commitments to storing your data and offering core services of our Office 365, Azure and Dynamics 365 products only within a particular geographic area – including Australia, via our datacentres in NSW and Vic.[17] So you know where your data is stored and enjoy the benefits of limited latency, remote access, and high level security to meet your obligations to protect the data from unauthorised use, access, disclosure or loss. That Microsoft is a foreign company is no regulatory hurdle – Microsoft is fully committed to providing cloud-based solutions for HCPs in Australia.

Steps you should take

Start by analysing the relative risks of moving to the cloud versus maintaining the status quo or adopting an alternative (e.g. hybrid private/community cloud). Ensure you understand the difference between speculative risks and the reality of risk exposure. Most HCPs find that, after reviewing their own security arrangements in detail alongside those offered by Microsoft, they are better able to meet compliance obligations by moving to the Microsoft cloud.

- Establish due diligence around contract terms.
- Ensure you understand Microsoft's security mechanisms, access controls, privilege management models, and operational diligence.
- Understand that, if required, Microsoft can provide compliance reports to verify that effective practices are in place and audited.
- Determine the geographic region where your tenancy is provisioned and data is stored at rest.

17. See the Data Processing Terms section of the Online Services Terms, available at https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx.

Most HCPs find that, after reviewing their own security arrangements in detail alongside those offered by Microsoft, they are better able to meet compliance obligations by moving to the Microsoft cloud.

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.

Regulatory considerations

The regulatory considerations for providing cross-organisational care in a cloud-hosted environment are substantially the same as those for providing care in any other environment.

The principal concern is that health information is collected only with the patient's consent, and used and disclosed only for the purposes for which it was collected, except in special circumstances. It must also be protected from unauthorised use, modification, disclosure or loss.

In some circumstances, compliance with these regulatory obligations is easier in a cloud-hosted environment than in on-premises or paper-based 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 HCPs can comply with their information security obligations.

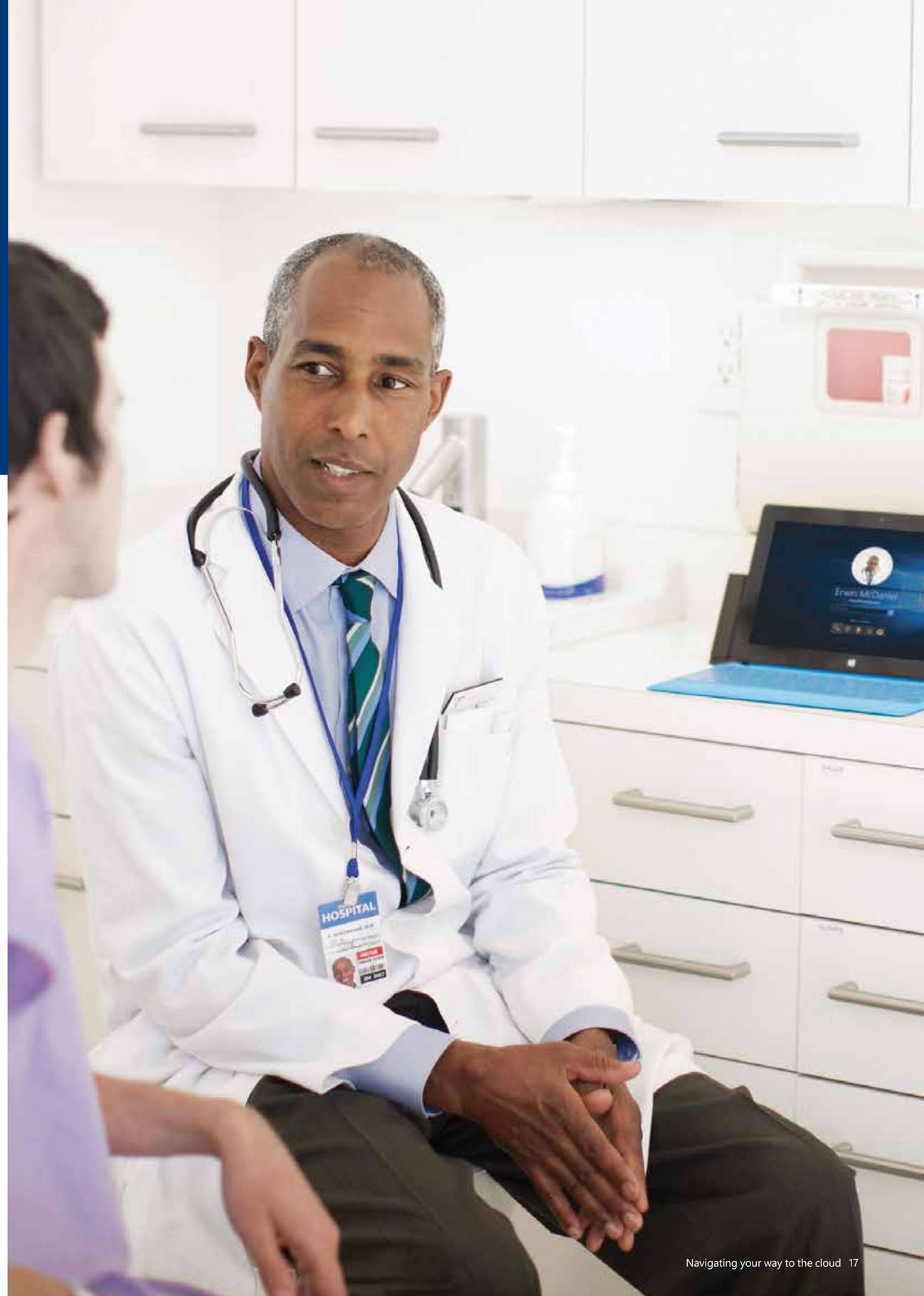
Hosting patient records in the cloud also facilitates team care arrangements by allowing different clinicians and HCP specialists to access a central and, in some cases, shared patient record so that all relevant information is available to them no matter where they are – even across organisations, if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

But it's not just about document storage systems. Practice management systems themselves can be delivered as a hosted service by installing them as an application 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 arrangement, the service organisation is responsible for physical and host security, and the practice management software organisation is generally responsible for security at the application level, so the HCP need focus only on data classification, client-side security, and identity and access management.

Steps you should take

- Identify who needs access to relevant systems and health information, and at what level, both within and outside your organisation.
- Consider incoming restrictions on the use and disclosure of patient records, and how you will reinforce those using cloud service features like role-based access controls and your own additional controls, as well as contractual measures between the participants.
- Decide who is responsible for responding to access and correction requests.



Using Azure to unlock data insights that help improve population health

Data-driven diagnostics have the potential to improve patient care, reduce costs, and optimise treatments and clinical pathways, as well as facilitate broad-scale research.[18]

The ability to analyse massive amounts of data is vital to the future of healthcare. But 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 health sector. 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 health information are no different in a cloud-hosted model than in a traditional on-premises model. Where the health information relates to the patient as an identifiable individual, misuse of that health information is a prohibited interference with their individual privacy. Information or data that does not relate to a particular individual whose identity can reasonably be determined is not personal information and there are no regulatory restrictions on the use of such information.

Under Australian law, personal, health or other sensitive information is not subject to any privacy regulations if it is de-identified so that it is no longer reasonably capable of identifying a particular individual (whether by that information alone, or in conjunction with other obtainable information). HCPs therefore do not need to comply with any additional regulatory requirements to use cloud-hosted analytics, such as those on Microsoft Azure, for research and practice improvement.

Microsoft can provide data analytics services as an optional value-add to our cloud services. These use aggregated and de-identified health information 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 health information 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 Services Terms.[19]

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 health information, personal information that is not sensitive information, or solely de-identified data;
- Whether medical research and analytics were each an express purpose of collection, a directly related and reasonable secondary purpose, or a purpose otherwise permitted under the Privacy Act such as research relevant to public health or public safety.

18. See Professor Sir John Tooke, Future of Healthcare in Europe (University College London 2012).
19. See the Cognitive Services section of the Online Services Terms, available at https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx.

Additional considerations

Due diligence and risk management

It is important to analyse in detail the risk associated with the cloud service you are considering, and compare that risk profile with the risk associated with maintaining the status quo or adopting an alternative, such as a hosted private cloud, community cloud or hybrid service. This is the only means by which conclusions on relative risk exposure can be made accurately.

Bear in mind that the public cloud typically enables customers to take advantage of the most advanced security capabilities and innovations, because public cloud services generally adopt those innovations first and have a much larger pool of threat intelligence data to draw upon. An example of this type of innovation in Microsoft cloud services is Advanced Threat Protection in Office 365, which provides a very sophisticated model to detect and mitigate previously unknown malware.

Our multi-tenant public cloud services are also designed to facilitate compliance by our most highly regulated customers, even if not all of our customers are subject to the same requirements.

Comparing risks

To understand the relative risk of the cloud service under consideration, you need to assess the risks associated with maintaining the status quo (which may involve continuing to run your application or servers on premises) and other alternatives under consideration, and compare those assessments with the risks associated with the proposed shared computing service. Our experience is that conducting a risk assessment of the status quo can reveal processes and controls that have not kept pace with evolving business practices and compliance requirements. Similarly, risk assessments that consider different alternatives (which may include a public cloud service on the one hand, and a hosted private or community cloud on the other) ensure you can make an informed choice, rather than relying on generalisations about the relative risk exposure of different options, which do not always withstand scrutiny.

Business continuity

There are no specific laws or regulations requiring HCPs to comply with resilience and business continuity measures. However, measures such as performing resilience testing and the provision of business continuity plans may be reasonable steps necessary in order for an HCP to comply with its requirements to protect the sensitive information it holds.

Microsoft's Enterprise Business Continuity Management (EBCM) program is based on the Disaster Recovery Institute International Professional Practice Statements and the Business Continuity Institute Good Practice Guidelines.

Our EBCM program applies across Microsoft's business and drives the development of business continuity plans (BCPs) for our individual cloud services in line with industry best practices. It also reflects the security controls of the production environment. For example, BCPs have been documented and published for critical Azure and Office 365 services. These BCPs set out roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives and Recovery Point Objectives. Plans are reviewed annually, at a minimum.

BCP testing

The BCP team (in co-ordination with the relevant cloud service team where appropriate) conduct testing of the business continuity and disaster recovery plans, per the defined testing schedule for each loss scenario at least annually. Issues identified during testing are noted and managed to a resolution.

Customer controls

In addition to our own rigorous program of recovery across our all our cloud infrastructure, we provide mechanisms for customers to control backup and recovery themselves. For example, in Office 365, document versions and email can be backed up and recovered by your in-house administrator. Azure Backup provides the ability to back up and restore virtual machines, and the Azure Import/Export service can be used to transfer large quantities of data residing in Azure Blob Storage to your on-premises installations. This gives you a great deal of control over how you choose to archive or even replicate data within your shared computing services.

Classifying data

It's important to evaluate the sensitivity of your data along with your backup and integrity requirements. You may well find that the mechanisms for backup and recovery within a service like Office 365 are entirely capable of addressing your requirements. But you can also extend that service by configuring additional backup, recovery or integrity mechanisms to meet compliance or other obligations.

Defining benefits

Infrastructure cost reduction is a commonly cited benefit of moving to the cloud, but there are many others, such as the ability to modernise service delivery, take advantage of improved mobile security, and redirect ICT staff to higher-value work.

One way to clarify your organisation's strategic intent is to classify the expected benefits of moving to the cloud as efficiency, effectiveness or performance benefits across the affected business areas. This helps to convey, concisely and clearly, the overall strategic intent to your stakeholders (including the Board and senior management). Of course, you should also conduct a thorough risk assessment. Understanding your organisation's internal context is also crucial, since the decision to move to the cloud does not occur in an organisational vacuum. There are structural, cultural and technological factors that need to be factored into your cloud adoption strategy, and those factors can be brought to the surface by asking questions such as those set out below.

Structural

- Which business units and processes will be affected by the solution under consideration?
- What resource limitations exist?
- How flexible is the organisation to structural change and resource reassignment?

Cultural

- Is the workforce culture receptive or resistant to technology innovation?
- What is the workforce awareness of risk and security process?
- What is the organisation's adoption of work-at-home and work-remote practices?

Technological

- What technology platforms are deployed within the organisation today?
- How will the cloud service be integrated with existing IT assets that will remain part of the overall architecture, particularly in areas like identity and access control, management and monitoring, and information protection?
- How modern is the existing technology experience of users within the organisation?

Appendix

Applicable health legislation by jurisdiction

Jurisdiction	Legislation	Regulators
Commonwealth	Privacy Act 1988 (Cth) My Health Records Act 2012 (Cth) Healthcare Identifiers Act 2010 (Cth) Health Insurance Act 1973 (Cth) Aged Care Act 1997 (Cth)	**Office of the Australian Information Commissioner (OAIC)** https://www.oaic.gov.au/ **Commonwealth Department of Health** http://www.health.gov.au/ **Chief Executive Medicare, Commonwealth Department of Human Services** https://www.humanservices.gov.au/
NSW	Health Records and Information Privacy Act 2002 (NSW) Health Services Act 1997 (NSW)	**Office of the New South Wales Privacy Commissioner** http://www.ipc.nsw.gov.au/ **New South Wales Health Care Complaints Commission** http://www.hccc.nsw.gov.au/
Vic	Health Records Act 2001 (Vic) Health Services Act 1988 (Vic)	**Office of the Commissioner for Privacy and Data Protection Victoria** https://www.cpdp.vic.gov.au/ **Victorian Health Services Commissioner** https://hcc.vic.gov.au/
ACT	Health Records (Privacy and Access) Act 1997 (ACT) Health Act 1993 (ACT)	**ACT Human Rights Commission** http://hrc.act.gov.au/ **ACT Health Services Commissioner** http://hrc.act.gov.au/health/
Qld[20]	Information Privacy Act 2009 (Qld) Hospital and Health Boards Act 2011 (Qld)	**Office of the Information Commissioner Queensland** https://www.oic.qld.gov.au/ **Office of Health Ombudsman Queensland** http://www.oho.qld.gov.au/
SA[20]	Health Care Act 2008 (SA) Premier and Cabinet Circular PC012	**Privacy Committee of South Australia** http://www.archives.sa.gov.au/content/privacy-committee-sa **South Australian Health and Community Services Complaints Commissioner** http://www.hcscc.sa.gov.au/
Tas[20]	Health Service Establishments Act 2006 (Tas) Personal Information Protection Act 2004 (Tas)	**Ombudsman and Health Complaints Commissioner Tasmania** http://www.ombudsman.tas.gov.au/making_a_complaint/your_privacy2 http://www.healthcomplaints.tas.gov.au/making_a_complaint/
NT[20]	Health Services Act 2014 (NT) Information Act 2016 (NT)	**Office of the Information Commissioner (Northern Territory)** https://infocomm.nt.gov.au/ **Health and Community Services Complaints Commission NT** http://www.hcscc.nt.gov.au/
WA[20]	Health Services Act 2016 (WA) Public Health Act 2016 (WA)	**WA Department of Health** http://ww2.health.wa.gov.au/ **Health and Disability Services Complaints Office** https://www.hadsco.wa.gov.au/home/

Note: Only the principal Act has been listed in each case. Subordinate legislation may also be relevant in particular circumstances.
20. The applicable legislation in Qld, SA, Tas, NT and WA applies only to public sector HCPs.

Microsoft