Microsoft

Five tactics for improving security and compliance in healthcare

Protecting data and staying compliant

Contents

01

Introduction

02

Strategising security and compliance

—Understanding the digital future of healthcare
—Microsoft helps you reimagine healthcare

03

Building blocks of security and privacy

—**Tactic 1:** Secure your data and network
—**Tactic 2:** Conditional access

04

Addressing compliance challenges

—**Tactic 3:** Assess the risks
—**Tactic 4:** Accountability and transparency

05

Choosing a cloud service provider

—Trusted cloud healthcare principles
—Evaluating cloud offerings: a checklist
—**Tactic 5:** Maintain data reliability to support business continuity

06

Summary

—Resources

01

Introduction

Modern digital transformation requires security transformation, too. As a healthcare leader, you frequently work with highly sensitive patient data. Each day, a greater variety and volume of this data is transmitted, stored and accessed in a plethora of mixed cloud environments. As you prepare to digitally transform, your organisation must also prepare to handle new risks, more sophisticated cybersecurity threats and a more stringent regulatory environment. *How can you protect sensitive data, stay compliant and do it at scale?*

As your organisation rethinks its approach to security and compliance, you may be wondering how to ensure confidentiality, integrity and availability without reducing productivity in a modern cyber world. Lucky you – today's technology already offers solutions that can protect your sensitive information. Upgraded technology empowers you to:

Protect infrastructure, data and apps effectively from internal and external threats.

Maintain control over who can access confidential data.

Balance data-breach prevention with granting authorised personal data requests.

Be accountable and transparent in your business processes.

Protect the integrity of data and ensure it remains accurate, complete and up to date.

Ensure your systems and data are always available to avoid interrupted services.

Upgrade to modern digital technologies and solutions to expand your business while detecting, containing and repairing potential vulnerabilities.

Where do you start?

This eBook reveals powerful insights about how to embrace these emerging opportunities. Here, you'll find an overview of the most important issues facing healthcare security and compliance, as well as five basic tactics to safeguard your data, successfully manage risk and meet compliance requirements now and in the future. Using these strategies, you can determine a path forward that best fits your organisation's digital transformation.

02

Strategising security and compliance

CONTENTS

Understanding the digital future of healthcare

Microsoft helps you reimagine healthcare

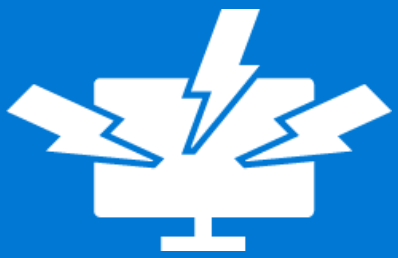
Understanding the digital future of healthcare

Healthcare is behind other sectors when it comes to its digital transformation efforts, primarily because few industries handle such complex and sensitive data environments. In your line of work, each new advancement (like genomics and digital medical images) generates an onslaught of highly sensitive data. You want trustworthy, reliable and modular technology solutions that can streamline digitising, managing and securing this information – ultimately saving you time and budget. More data means more storage requirements, heightened legal obligations and higher costs – a vulnerable ecosystem open to cyberattacks.

You also want to integrate your data with current IT and health technologies that often run on different platforms – all of which need to follow the same security and compliance regulations. Because of this historic surge in connected Internet of Things (IoT) devices that support innovative virtual health and telemedicine solutions (like wearables, smart beds and portable medical technologies), data security is more critical than ever.

Healthcare organisations that understand, and capitalise on, this opportunity are already transforming operations. They've developed a new generation of data-driven health processes and solutions that enable them to drive healthcare improvements while optimising costs.

More sophisticated attacks



One in three healthcare organisations have suffered a cyberattack.

Read more ›

Need to secure data

A whopping 408 USD: the per capita cost of a health data breach.

Read more ›

Microsoft helps you reimagine healthcare

Healthcare needs a new IT model that can improve the patient experience, enable collaboration beyond firewalls and improve organisational outcomes – all without compromising security and compliance standards.

Your organisation will benefit greatly from an integrated business and technology strategy aimed at achieving these goals. Your strategy should be as unique as you are, and cover each corner of digital transformation:

People (your culture)

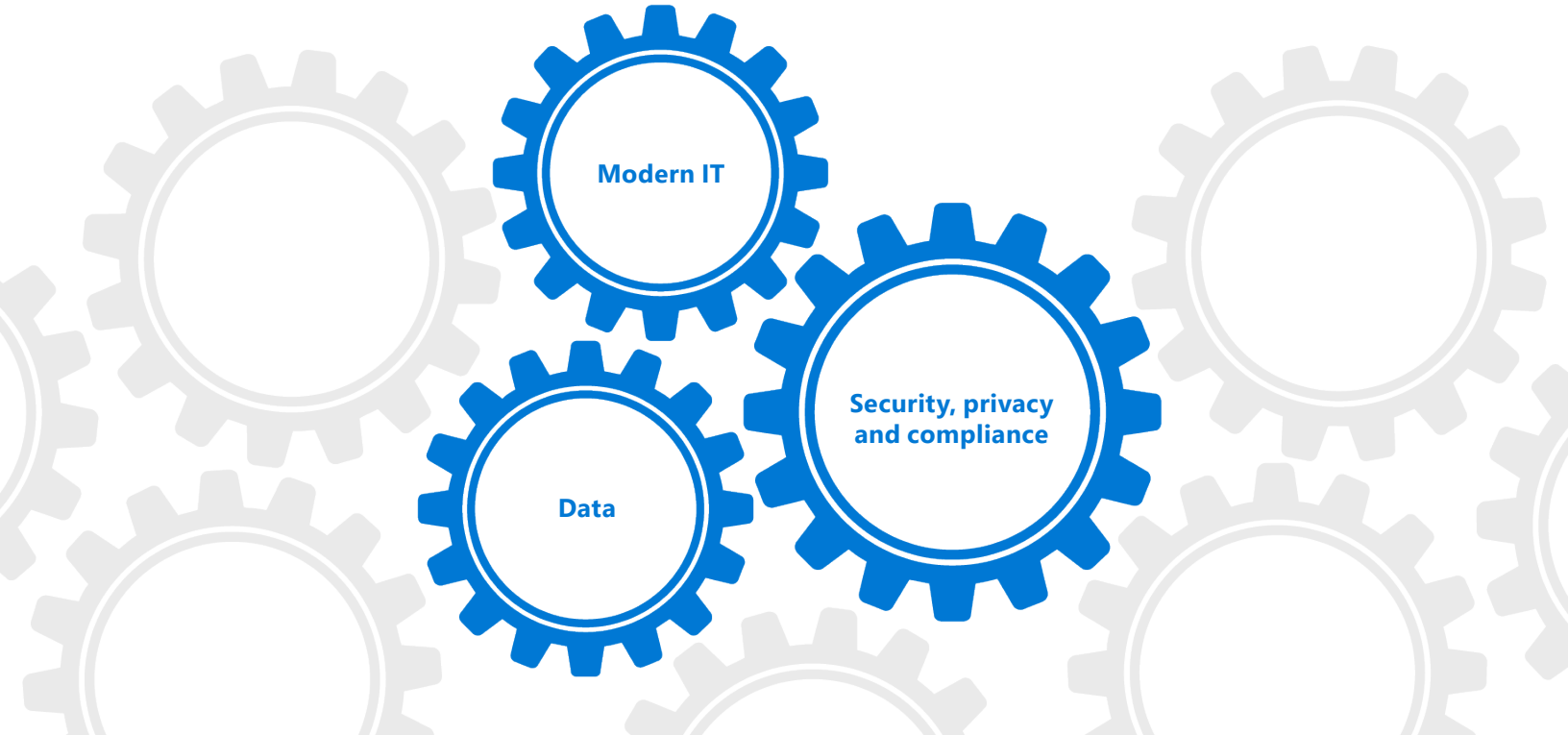
Processes (the approach you take)

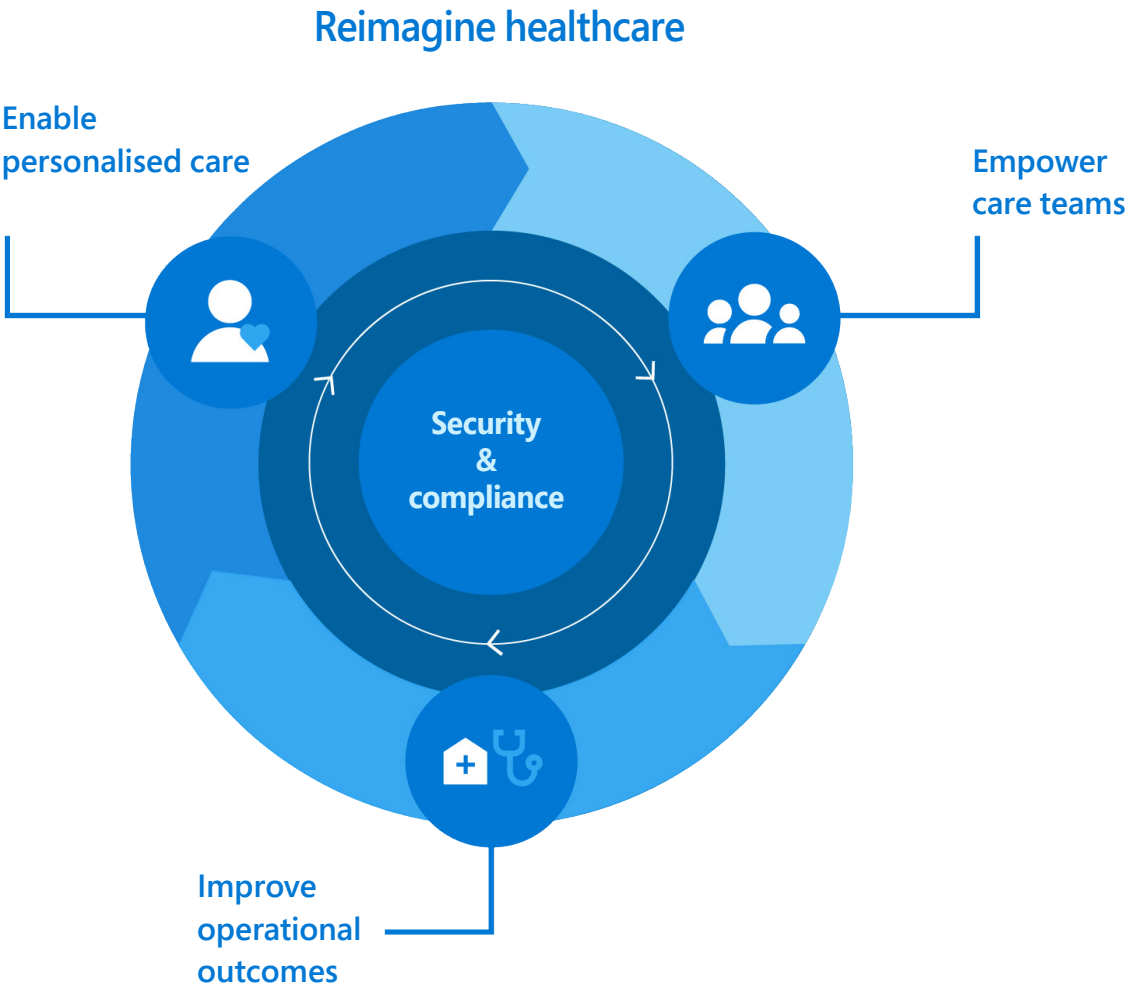
Technology (the tools that make it all possible)

Take advantage of modern technology like the cloud, AI and data aggregation (IoT, genomics, lifestyle and research) with the right mix of control and security. Strike a balance between modern IT, data and security to minimise risk and enable a strong compliance posture.

Microsoft proposes a new model with strategies aimed at empowering your care teams, improving clinical and operational outcomes, and advancing precision healthcare – with a careful focus on people's privacy and security. With this model, you can design and deploy new digital experiences and products that are streamlined and secure across your extended value chain. This approach improves patient care and provides secure and well-connected tools. Your teams will easily collaborate with payors, outside clinical specialists and patients. You'll also streamline the healthcare process and improve outcomes by turning data into actionable insights, in almost real time – all without compromising security, privacy or compliance.

Source >





Microsoft commissioned Frost & Sullivan (a global research and consulting firm) to evaluate Microsoft 365 from a healthcare point of view, and they discovered that the most common pain points clinicians face regarding electronic clinical messaging include issues related to security and improving how clinical staff can collaborate better in a convenient and seamless way. Microsoft Teams directly addresses the top challenges facing healthcare providers with a modern, chat-based collaboration tool that doesn't require compromising on security and compliance.

"Based on our research, Microsoft Teams directly addresses the top challenges facing healthcare providers in electronic messaging in hospitals and health systems."

Greg Caressi, Frost & Sullivan
Source ›

03

Building blocks of security and privacy

CONTENTS

Tactic 1: Secure your data and network

Tactic 2: Conditional access

In this modern marketplace, it is critical to embed security and privacy into all aspects of digital interaction. That includes ensuring the accuracy of technology foundations with precise measures to address data security and privacy. For healthcare leaders, there is even greater moral and regulatory responsibility to carefully oversee captured data and control access to sensitive healthcare information. Healthcare organisations should also consider other types of collected data that are subject to privacy requirements.

The culture promotes collecting increasing amounts of patient data, which means health organisations must revisit data strategies, focus on data collection and ensure that privacy-by-design and security-by-design principles are upheld. Privacy is no joke, you're promising that personal and sensitive health information – and corporate data – is used, protected, controlled and destroyed legally and properly. By exploring new, data-driven business models, you can tackle how to manage security and privacy effectively, and stay ahead of the curve.

As technology advances, so do cyberthreats. The impact of data vulnerabilities and breaches can be costly and damaging – both to your organisation and your healthcare consumers. Cybercriminals are targeting health organisations more frequently, so it is vital that you keep patient information and other sensitive data secure while preserving privacy.

Modern security demands protection for organisational data, apps, devices and patient information is ensured in all forms.

Consider using some new tactics to address security and privacy gaps.

"Despite increased investments by healthcare stakeholders, cyberattacks in the healthcare industry will double in 2018. This makes it essential for health authorities to develop risk management solutions."

Wes Wright, former Corporate Chief Technology Officer, Sutter Health

Source ›

Tactic 1: Secure your data and network

Start with these questions

Can you effectively secure your infrastructure, data and apps from internal theft and targeted cyberattacks?

Do you know who accesses your data and apps at all times?

Do your clinicians have secure access to the systems, apps and resources they need – even if they are remote or travelling?

Can your organisation quickly and broadly apply your identity and security policies across all devices and apps?

Key benefits and outcomes

After all is said and done, digitally transforming will help you:

Minimise risk while sharing and integrating patient data securely across different medical systems.

Boost security and privacy, and enjoy peace of mind.

Minimise cybersecurity incidents and potential data loss.

Better protect your sensitive data across endpoints (both mobile and apps).

Secure data and keep it under your control.

A path forward

You have a moral imperative to be stewards of sensitive health data and apps. Your strategy should focus on automatically identifying and protecting sensitive information, and preventing its disclosure.

Add a layer of data governance policies and protection across systems, devices and apps, both on-premises and in the cloud. Use your cloud provider's platforms, solutions and tools to create data asset security policies, and control those policies and data access.

How can it help your organisation?

You'll be able to identify and retain important information, review documents efficiently and prevent accidentally sharing sensitive information – all while making it easier to eliminate trivial, redundant and obsolete data. Rest assured that if a device is lost or compromised, it can be remotely wiped, making sure that patient's sensitive information remains secure. Our built-in tools monitor health apps and data sets to prevent malicious access and quickly detect and respond to cyberthreats.

CASE STUDY >

Sutter Health: Strengthening patient care while addressing concerns around security

Employees at Sutter Health needed a unified approach to technology management, security and communications. Sutter Health invested in deeply integrated technology by rolling out Microsoft Office 365. The built-in security features of Office 365 Advanced Threat Protection provided scalability, so Sutter Health could increase its cyber defence and data protection while eliminating the need for network drives.

Facilitated by Microsoft Teams and Office 365 Video, dialogue and collaboration among a diverse healthcare population became simpler. They securely accessed and used Sutter Health-authorised apps whenever the need arose. Ultimately, employees escaped their screens to spend more time with patients.

"Office 365 impressed us as a standard platform that would take care of many of our unique concerns as a healthcare provider. Chief among these are security and compliance. We use Intune – part of Enterprise Mobility + Security – to manage some 65,000 mobile devices, so our clinical and business partners can access and use Sutter Health-authorised apps anywhere they need to. We expect to see productivity at a whole new level."

Wes Wright, former Corporate Chief Technology Officer, Sutter Health

Tactic 2: Conditional access

Start with these questions

Can you currently protect sensitive information across identity, apps, data and devices, ensuring that the information is available for the intended recipient?

Can you control access to your data across all PCs, tablets and smartphones used by the people inside and outside of your organisation – or the devices visitors and patients want to use?

Can you control human error – including social engineering attacks, phishing emails and spoofing – which can allow cybercriminals to steal credentials and identities?

Key benefits and outcomes

Secure and protect sensitive health information.

Defend users, devices and data.

Control access to apps based on specific conditions.

Reduce the risk of a data breach and loss.

Establish standard security best practices and industry compliance.

What should your strategy be?

In today's mobile- and cloud-first world, you need real intelligence that spans critical end-points, so you can:

Permit and restrict data access based on the device risk level to limit potential attack surface.

Define security conditions that let apps run and access patient information on your network.

Enforce policies that stop apps from running until a device is compliant.

Enable real-time notifications to detect data breaches by continuously scanning devices, apps and services.

How can it help your organisation?

With a controlled and conditional access approach, you can better see user access points and activity. You'll protect your users and critical health information by ensuring that only secure devices have access to apps. These controls will enable you to limit and manage data access from a variety of devices and support different use scenarios based on location, device type and network.

Office 365 allows or blocks people from accessing resources under certain circumstances that you can choose.

CASE STUDY >

Health provider boosts security and manages all devices with data protection and identity management features

Carinova prioritised data protection and compliance with healthcare standards, but still found gaps when safeguarding information. Employees work with personally identifiable information (PII) that's highly sensitive (like electronic health records) and falls under regulations like the European Union General Data Protection Regulation (GDPR) privacy laws. Carinova arranged for a Microsoft Software Asset Management (SAM) evaluation of its IT environment.

The SAM team suggested ways to enhance the benefits of their integrated cloud platform by adding visibility, simplified management and scalable device/identity management. Carinova adopted Microsoft Office 365 cloud technologies to manage all mobile devices, which added the data protection and identity management features needed for GDPR compliance.

Carinova expanded its identity management with Microsoft Office 365 to track the apps that employees install and use. Carinova can now identify shadow IT and dark data – and see a clearer picture of unapproved app use in order to protect sensitive information better.

"Based on the SAM cybersecurity engagement, we decided to adopt Microsoft 365 cloud technologies to manage all our mobile devices, with the data protection and identity management features we need for GDPR compliance."

Ton Kuiper, IT Specialist, Carinova

04

Addressing compliance challenges

CONTENTS

Tactic 3: Assess the risks

Tactic 4: Accountability and transparency

While advances in healthcare IT are currently promising, concerns about compliance make some healthcare organisations anxious about adopting modern technology solutions. Compliance requirements – especially in a highly regulated industry like healthcare – can be difficult to interpret, labour-intensive to implement and tough to monitor.

Many health organisations will need to thoroughly re-examine their data flows, stores and privacy processes.

How can you be sure that a solution is trustworthy?

Certifying a solution's reliability is crucial. Ensuring the privacy of personal information isn't just a moral issue, but a legal one too. You'll want to ensure that all patient and organisational data complies with ever-changing standards and regulations.

So, in the face of compliance challenges, you might struggle to determine where and how to begin your digital transformation journey. How can you balance meeting regulatory mandates while securing infrastructure and patient information?

You can start with the following tactics.

"We look at compliance as people, process and technology. You have to have all three in order to be compliant."

Nancy Wilson, VP of Privacy and Compliance, Lumen21

Source >

Tactic 3: Assess the risks

Start with these questions

Do you have a process to assess, protect and manage personal and private data with appropriate risk control? Are these mechanisms automated and kept up to date?

Can you assess your current compliance risk, and do you have IT strategies to improve your compliance posture?

Can you prevent unlawful data use, accommodate personal data requests and receive breach notifications promptly?

Key benefits and outcomes

Assess and manage compliance risk

Meet industry compliance (HIPAA, GDPR, local privacy laws, etc.)

Stay up to date with changing regulatory requirements

What should your strategy be?

It can be challenging to know your current state of compliance, not to mention the expense of figuring out what to do about it. You can manage all compliance from a single place and see how your compliance posture stacks up against evolving regulations in real time. With a single view, you can implement controls that correspond to varying levels of risk.

How can it help your organisation?

With this strategy, you'll proactively reduce compliance risk and protect information while enabling technical and process requirements around data. You'll also improve productivity, rather than slow things down, by adding these layers of protection.

Stay ahead of all your tasks so that you can assign responsibilities to the right employees. Plus, by strengthening your process accountability, you'll further ensure compliance.

CASE STUDY >

Abrona accelerates GDPR compliance and proceeds faster with its digital workplace goals

Abrona wanted to track regulatory compliance activities related to its cloud services. They decided to deploy Compliance Manager, a cross-Microsoft Cloud risk assessment tool, and gained new insight into their data protection and compliance stature. Because they are in Europe, the effects of GDPR were imminent. However, by using Microsoft's information protection solutions like Compliance Manager, they now have an efficient way to handle compliance holistically.

Abrona made significant headway with its compliance activities for GDPR. Information and Communication Technology Department staff use the digital checklists to see how to improve their compliance posture within the Office 365 environment.

"Today, we can assure our Board of Directors that we are taking all required steps to deploy a highly secure and compliant Office 365 solution. We consider Compliance Manager a fantastic product. Compliance Manager adds great additional value to Microsoft Cloud services by providing insights into the relationships between regulation, processes and technology."

Nick Postmas, IT Manager, Abrona

Tactic 4: Accountability and transparency

Start with these questions

Do you have audit-ready tools in place to track data with the necessary transparency and accountability in every business process?

Do you have a system that can detect, locate and bring accountability to personal and health data?

Key benefits and outcomes

Adhere to corporate governance policies.

Automate remediation and investigation, and reduce the burden on your team.

Gather improved insights about health operations.

Manage and monitor your processes in real time.

What should your strategy be?

Streamline your compliance and reporting processes. Coupled with modern technologies like AI and machine learning, data can determine procedures – which extends to both operations and clinical settings. This approach can help you move faster and work more efficiently when notifying authorities about personal data breaches, obtaining appropriate consents for processing data and maintaining detailed internal records. Add data classification, labelling and encryption capabilities for stalwart protection across devices, apps, cloud services and on-premises solutions.

How can it help your organisation?

With a streamlined approach, you'll increase transparency and control data flow for both personalised care and precision health processes, which makes it easier to trace and control sensitive data across devices and apps. Effortlessly investigate, hold and refine data relevant to regulatory investigations, medical research or malpractice actions, and reduce the time and efforts required for discovery.

CASE STUDY >

MEDNAX manages business processes and empowers workers with administrative controls

To empower their employees to succeed in a modern workplace, MEDNAX turned to Microsoft Office 365 cloud services. MEDNAX deployed their chosen scheduling solution, Microsoft StaffHub. StaffHub works closely with the other Office 365 communication and collaboration services, which makes it easy for employees to establish streamlined workflows. Employees use SharePoint Online (part of Office 365) to combine a highly secure collaboration framework with improved collaboration. Coordinators and screeners also take advantage of the secure file-sharing capabilities to access hospital policy and procedure documents quickly. Coordinators can now set schedules, and then assign appropriate levels of access for screeners.

By using StaffHub, coordinators achieved greater control over who could access work calendars, and therefore gained a strengthened security posture.

"With Microsoft cloud services, we can provide a highly secure work environment. We found the rich security controls in Office 365, such as Exchange Online Protection, to be far better than any offered in comparable systems. Moreover, we no longer see improvised workarounds for staffing, which means overall administrative efficiency is up."

Darren Handler, Director of IT Research and Development, MEDNAX

05

Choosing a cloud service provider

CONTENTS

Trusted cloud healthcare principles

Evaluating cloud offerings: a checklist

Tactic 5: Maintain data reliability to support business continuity

Trusted cloud healthcare principles

Cloud platforms enhance privacy and security by allowing healthcare organisations to access expertise and invest in these areas without starting from scratch. Because your organisation likely prefers a tailored approach, you need cloud service providers focused on the healthcare market that offer custom networked data and interoperable solutions.

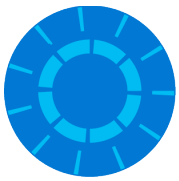
But what about trust? To ensure that providers deliver reliable cloud services and technologies, check that they follow four foundational principles:

Security

Your data confidentiality, integrity and availability are well protected.

Transparency

You can see how your data is handled and used in real time.



Compliance

Your content is stored and managed in compliance with applicable laws, regulations and standards.

Privacy and control

No one can access your data if you don’t approve it. You maintain control.

Evaluating cloud offerings: a checklist

Health organisations need cloud services that are not only powerful but secure and easy to use. What else should you look for, though?

Here's a checklist to use while evaluating cloud service offerings based on the four foundational principles:

Security

- Are there tools to secure identities and conditional access to your corporate resources and data?
- Does the provider ensure security for your infrastructure across all endpoints?
- Are you continuously kept up to date with security patches and is your system automatically safeguarded from the latest cyberthreats? Does the provider offer technologies, like machine learning, to detect, contain and remediate malware?
- Can you certify that devices connected to your cloud are free from viruses and malware? What happens if devices are lost or stolen?
- Is there a secure data network to encrypt information as it travels between devices and cloud datacentres (or moves within datacentres)?

Transparency

- Are they transparent about datacentre locations and where they store your data?
- Do you know how your data is protected, where it came from, and that it hasn't been tampered with?
- Do you know who can access your data and under what circumstances, and how it is protected, transferred and deleted?
- Do you know where and how electronic protected health information (ePHI) is stored, moved and handled by the cloud vendor?
- Did they establish clear transparency and precision in the contract agreements regarding security risks, roles and responsibilities?

Evaluating cloud offerings: a checklist

Compliance

- Does the provider have certifications proving they comply with health security and privacy regulations in the countries where you operate?
- Did they sign a HIPAA business associate agreement or other required contractual amendments?
- Are they keeping up with the latest health regulations?
- What's their history when it comes to compliance leadership?
- Do they perform in-depth audits of compliance control implementation and effectiveness?
- Can you ensure that each user interaction with your data and services is auditable?

Privacy and control

- Can you ensure that they won't scan your data for marketing purposes or treat it as a product to sell to others?
- In the public cloud, do they offer logical isolation and control for each customer's cloud data?
- Will they send clear communications about what they are and aren't doing with your data?
- Does the provider's cloud service agreement ensure that they can furnish all required data service levels in disaster recovery issues?
- Can they offer you continuous services without disruption?

Once you've found a trusted cloud service provider, how can you maintain data availability and reliability in your organisation? Here's one tactic to try.

Tactic 5: Maintain data reliability to support business continuity

Start with these questions

Are your healthcare systems and data always available and delivering information promptly?

Are your systems and data protected from ransomware, distributed denial-of-service (DDoS) attacks and other attacks on availability?

Are your systems safeguarded against data loss or interruptions, including unpredictable events like natural disasters and fire?

Did your provider enable a resilient infrastructure that can easily be integrated with your organisation's current and future operations?

Key benefits and outcomes

Maintain business continuity with data resiliency.

Avoid unexpected disruptions.

Eliminate data risks while ensuring data integrity and availability.

Comply with industry data security and business continuity standards.

What should your strategy be?

A disruption to infrastructure services and your mission-critical business apps can put patient lives at risk and reduce revenue and productivity, but don't worry – you can address this risk with built-in business continuity.

Your data can stay available across all systems, and you'll establish resiliency with copies of your data and apps in two sites. This way, you can ensure that if one location goes down, users automatically and seamlessly switch to the other site with minimal or no loss of data or productivity.

How can it help your organisation?

With this strategy, you can ensure that patient data is available with continuous connectivity and business continuity. You'll provide timely, reliable access to information in order to make data-driven decisions. Plus, you can protect operational services in the event of a service disruption.

CASE STUDY >

Peace of mind with reliable and trusted cloud infrastructure

Nuance needs their speech solutions to be available at all times, so they use a variety of Microsoft Azure services that meet this demand. For high-availability uptime requirements, Nuance deployed speech solutions in an active-active configuration in two Azure datacentres. Nuance is using the Azure Traffic Manager to intelligently route traffic to the closest datacentre based on network response times, which ensures that doctors have an optimal experience.

Nuance also uses Azure Traffic Manager to seamlessly route traffic between datacentres – facilitating maintenance and updates without any downtime.

"Since moving to Azure, we've dramatically improved our uptime commitments. Hospitals never close, so our previous maintenance windows were always a hassle for our clients."

John Vasicek, Vice President of Cloud and Mobile R&D, Nuance Communications

06

Summary

Healthcare organisations need to achieve digital transformation with complete peace of mind. With the evolution to a more data-driven, mobile and collaborative environment comes new vulnerabilities, security issues and increased regulation. To thrive in this privacy-focused era, you need to have a unified business and technology strategy to achieve the right equilibrium between modern IT digital transformation, data and security to minimise risk and enable a strong compliance posture. Microsoft 365 can help health organisations meet or exceed regulatory compliance needs, reduce compliance risk and serve as trusted stewards of sensitive health data. We embrace our responsibility to create a safer world that enables your organisation to transform digitally. This includes privacy, as well as making sure that you have control over your data and that you know what's happening with it. This transparency ensures that you can achieve compliance objectives.

With careful planning, a thorough assessment and the right selection of processes and services, healthcare organisations can simplify their privacy, security and compliance journey. To learn more about how to do a risk assessment for your healthcare organisation, visit the Microsoft Trust Center.

Visit Microsoft Health ›

Visit Microsoft Service Trust Portal ›