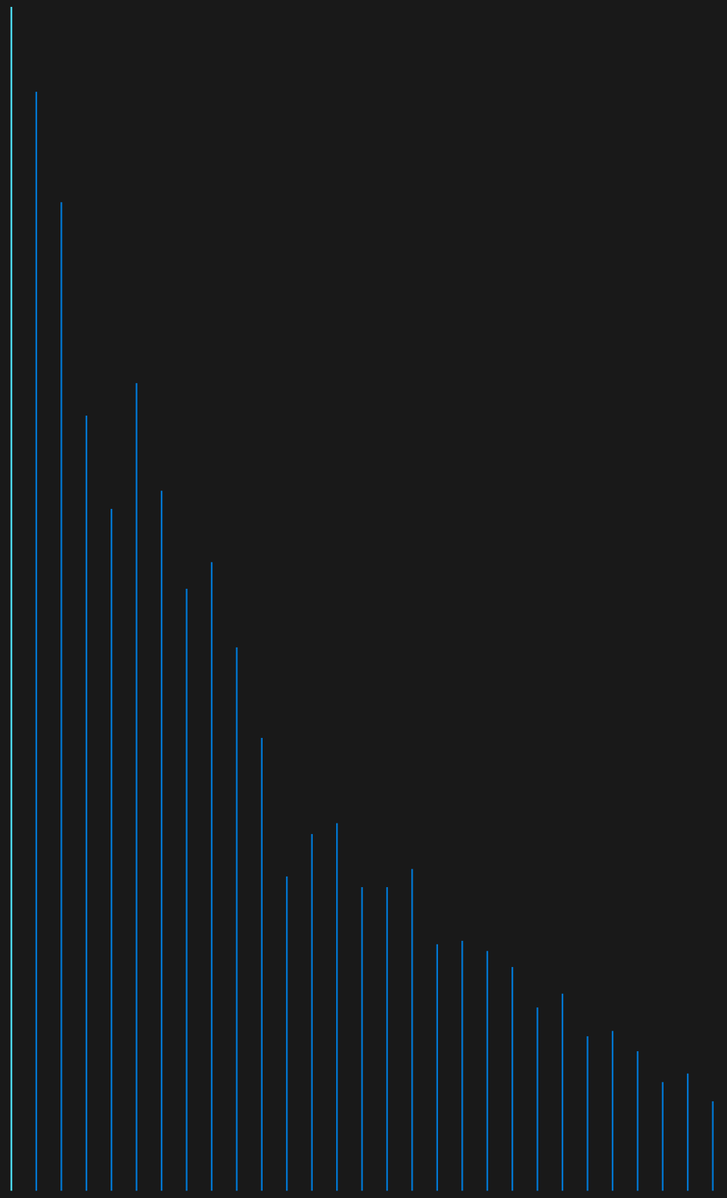
Microsoft

The Future of Healthcare Security and Compliance

Principles for maintaining data integrity in the cloud

Contents



01
Introduction

There has been an explosion of healthcare data due to the surge in digital healthcare services over the past year

Unlocking the value of this data requires industry-wide digital transformation. While this digital transformation is leading to better outcomes in healthcare—such as more personalized patient experiences and more streamlined operations—there is also the potential for increased security risks.

Hackers are becoming more sophisticated

Cybersecurity attacks are proliferating. The healthcare industry is a particularly attractive target to hackers who know that threatening to divulge highly sensitive patient information could result in big ransom paydays.

These cybersecurity attacks target healthcare organizations of all sizes, not just large companies. Security compromises can come from malicious outside threats as well as internal security breaches, such as when an employee opens what seems like an innocent email attachment and the organization's data is compromised.

Digital transformation is essential in healthcare

Providers can now meet patients' changing needs and their desire for more personalized care and real-time health information. But innovation cannot come at the cost of compromising sensitive patient information. Healthcare providers can now implement both innovative practices and a highly secure infrastructure to maintain an edge in the future.

The right cloud technology makes it possible for healthcare providers to embrace innovation with minimized risk. Cloud-enabled technology, from a trusted partner, can ensure that organizations embrace the innovations made possible by the data explosion while still maintaining robust data security.

Microsoft Cloud for Healthcare is your trusted partner

Microsoft Cloud for Healthcare is the only cloud platform with integrated capabilities that enrich, normalize, and unify protected health information (PHI). This industry-specific cloud solution protects valuable health information while enabling customers to support their compliance and making health data more accessible to the right users. Microsoft Cloud for Healthcare enables secure, interoperable data access and scalable AI to protect health information across the care continuum. A robust partner ecosystem extends the value of the platform with additional solutions to address the most urgent challenges the healthcare industry is facing today.

Microsoft Cloud for Healthcare enables real-time insights for agile decision-making.

See how Microsoft Cloud for Healthcare can accelerate innovation

---

Upgraded technology empowers you to:

- **Protect** infrastructure, data, and apps effectively from increasingly sophisticated cyberthreats.
- **Easily access** healthcare data.
- **Remain** compliant and secure.
- **Maintain** control over who can access confidential data.
- **Balance** data security with controlled permissions.
- **Become** transparent in your business processes.
- **Protect** the integrity of data and ensure it's never shared or sold.
- **Ensure** your systems and data are always available to avoid interrupted services.
- **Upgrade** to modern digital technologies and solutions to expand your organization while detecting, containing, and repairing potential vulnerabilities.

02
Strategizing security and compliance

Understanding the digital future of healthcare

Healthcare is behind other industries when it comes to digital transformation, primarily because few industries handle such complex and sensitive data environments.

In healthcare, each new advancement (like genomics and digital medical images) generates an onslaught of highly sensitive data. More data means more storage requirements, heightened legal obligations, and higher costs. Organizations need robust technology solutions that can streamline information, ultimately saving time and budget.

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

Healthcare organizations that understand and capitalize on this opportunity are already transforming operations and improving business outcomes as a result.

A healthcare data breach comes with a hefty price tag—to the tune of

$7.13 million

on average.[1] That's up more than 10 percent from 2019, when the average data breach cost healthcare organizations $6.45 million.[2]

On average, **it takes the healthcare industry 236 days to identify a breach and 93 days to contain a breach**—nearly two months longer than other industries.[1]

Microsoft Cloud for Healthcare helps you identify and block potential data leaks.

Learn how to prevent costly breaches with Microsoft Cloud for Healthcare

CASE STUDY: IMPROVING PATIENT AND EMPLOYEE EXPERIENCES

How St. Luke's University Health Network protects patient data

St. Luke's University Health Network (SLUHN) has clear priorities when it comes to its digital health transformation: improve patient and employee experience through highly secure health team communications.

Through the deployment of Microsoft Cloud App Security, SLUHN has already gained visibility into its third-party apps, solving a major pain point. "One of our challenges prior to deploying Cloud App Security was detecting shadow IT," says Erin Boris, Information Security Strategic Specialist at SLUHN. "Gaining that visibility through Cloud App Security helps us with software inventory, app rationalization, and most importantly, data loss prevention.

Cloud App Security has already discovered unsupported apps, a huge help in closing down potential data leaks. We have the ability to block unsupported cloud applications with one click, which we've never had before."

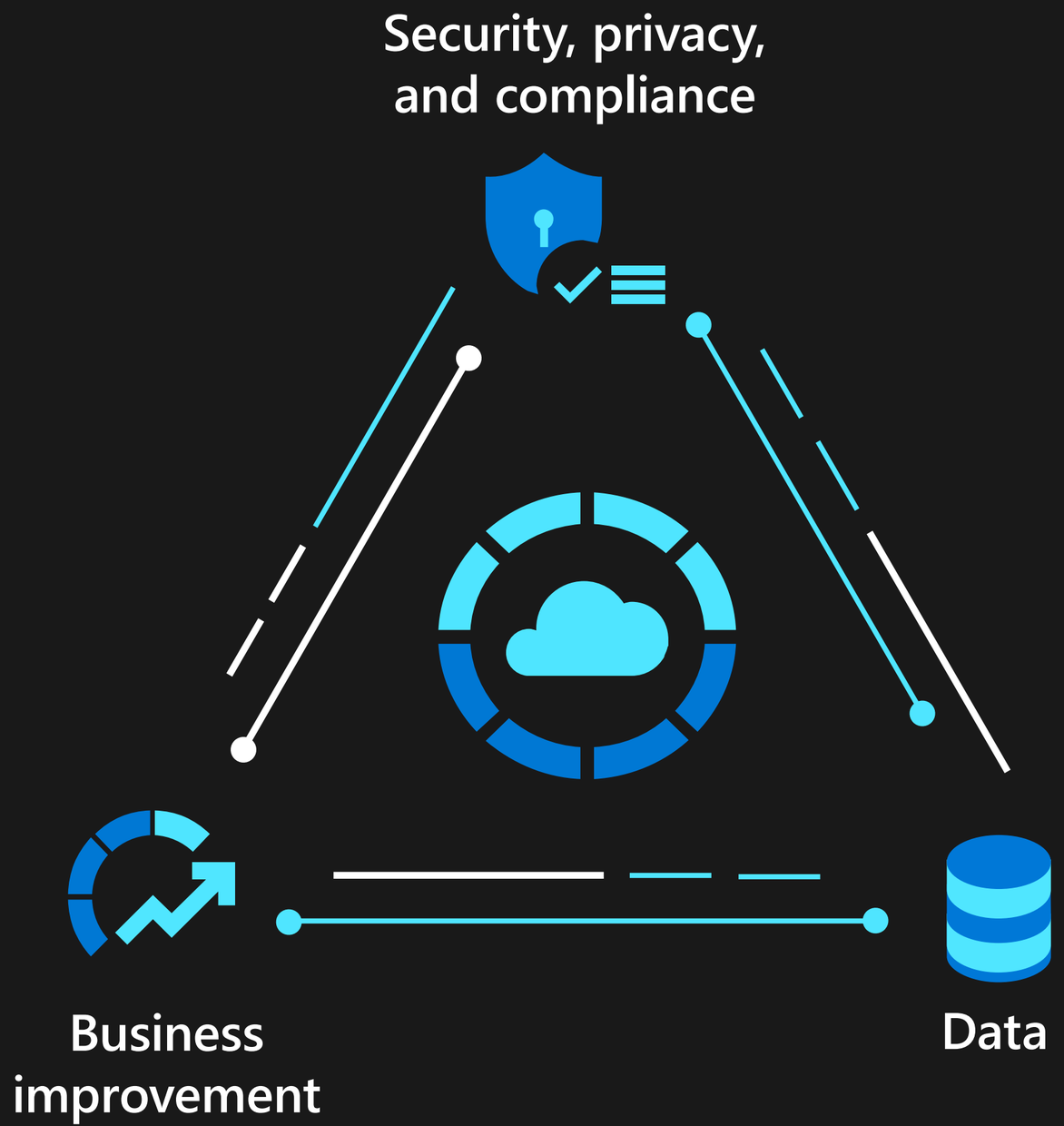
Learn more about how St. Luke's protects patient data

> At the end of the day, we can say to the patient, alongside the quality of health services you receive, protecting your data is the most important thing to us. Thanks to Microsoft 365, that's one more way we can differentiate the culture of care at St. Luke's.
>
> **David Finkelstein**
> Chief Information Security Officer,
> St. Luke's University Health Network

Microsoft is your trusted partner in cloud security

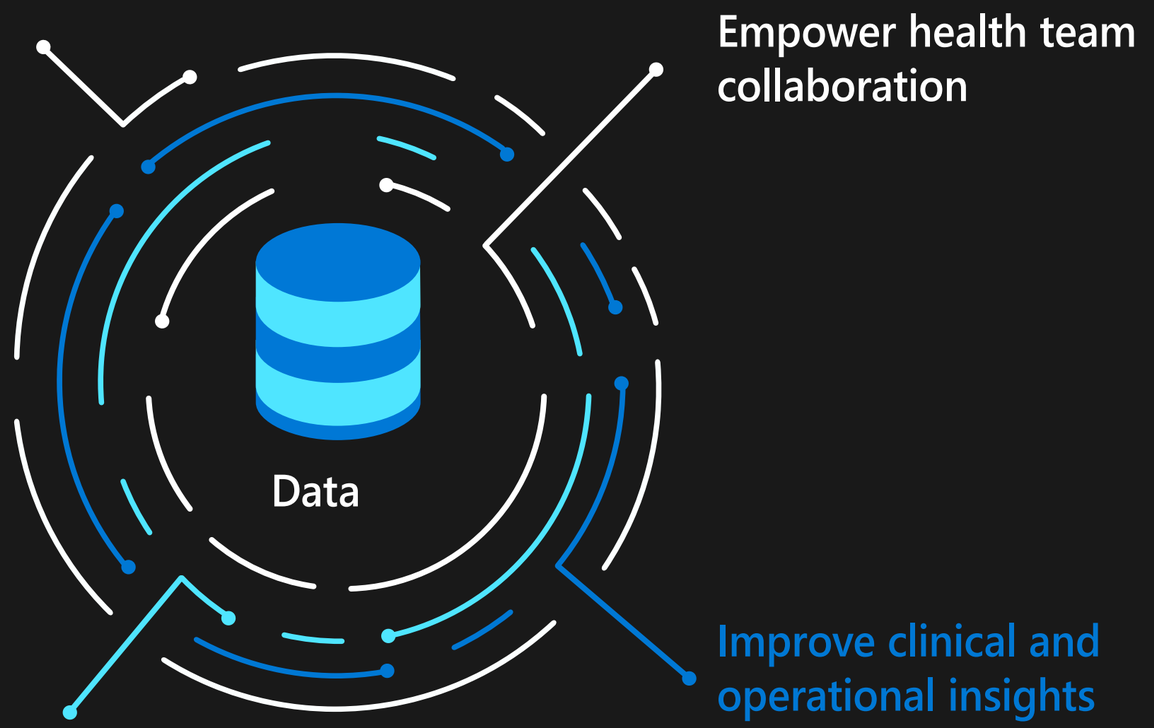
Every day, healthcare organizations are managing increasingly vast volumes of data. Moving to the cloud introduces the potential for greater risk if it's not handled correctly.

To help maintain data privacy and compliance, it's vital to work with a trustworthy service provider. The Microsoft holistic approach is designed to build trust by providing deep security and helping customers support compliance efforts. Microsoft's expertise in supporting customers to meet their compliance needs spans Health Insurance Portability and Accountability Act (HIPAA) business associate agreements for business cloud services and more.



Reimagine healthcare

In this digital age, anyone with an internet connection is a target for fraud. Due to the nature of sensitive protected health information and personally identifiable information, healthcare providers face increasingly complex fraud challenges and cybersecurity workforce issues.



"Without taking action to implement data security, given enough time, the chances of being breached becomes 100%. … Thanks to heavy investments Microsoft has made in security, compliance and auditing … Office 365 and Teams users can leverage built-in security and compliance features … to combat the constantly evolving cyber-security attacks everyone faces in healthcare and beyond."[3]

HIPAA Compliance Microsoft Office 365 and Microsoft Teams report

CASE STUDY: DATA AUTOMATION IN A SECURE ENVIRONMENT

How Cerner integrated Microsoft 365 to create a strong security foundation

Cerner's health information technologies connect people and systems at more than 27,500 contracted provider facilities worldwide. Recognized for innovation, Cerner offers solutions and services for healthcare organizations of every size. While its products were innovative, its internal practices were more manual. Until recently, Cerner associates relied on email to send documents back and forth and dealt with time-consuming versioning issues.

As most of Cerner's services include the care and management of its customers' healthcare data, the security of that data is paramount. "As we are entrusted with our clients' information, maintaining a secure environment is essential to our ability to deliver on that trust," says Bill Graff, Chief Information Officer at Cerner. "Microsoft has made tremendous investments over the last few years in its security capabilities. We didn't want security services that are bolted on; we wanted security from the start. Microsoft 365 E5 delivers the latest interoperable security services we need."

Learn more about how Cerner prioritizes security and compliance

> [We] have to reassure our clients that we can process their health information within our cloud-based environment in a manner that prioritizes safety and compliance. Microsoft has a great reputation, and we are confident that we are moving in the right direction with Microsoft 365.
>
> **Marc Elkins**
> Vice President, Associate General Counsel and Chief Compliance Officer, Cerner

03
Building blocks of security and privacy

In this modern marketplace, it's critical to embed security and privacy into all aspects of digital interactions

That includes ensuring technology foundation accuracy with precise measures to address data security and privacy. For healthcare leaders, there's an even greater moral and regulatory responsibility to carefully oversee captured data and control access to sensitive healthcare information. Healthcare organizations should also consider other types of collected data that are subject to privacy requirements.

Our culture promotes collecting increasing amounts of patient data to create a more personalized patient experience. Health organizations must revisit data strategies, focus on data collection, and ensure that privacy-by-design and security-by-design principles are upheld. 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—to both your organization and healthcare consumers.

Cybercriminals are targeting health organizations more frequently, so it's vital that you keep patient information and other sensitive data secure while preserving privacy. Modern security demands that protection for organizational data, apps, devices, and patient information is ensured in all forms.

While there has always been a need for tight security in the healthcare industry, the data explosion and ever-changing health landscape have exponentially increased that need. Vaccine fraud is becoming an ongoing risk. Issues of patient privacy and the potential for fraud must be proactively combatted to protect public health.

3x

Cyberattacks in the healthcare industry are predicted to triple year over year from 2020 to 2021.[4]

Microsoft Cloud for Healthcare helps you swiftly identify and resolve security attacks.

Keep data protected with Microsoft Cloud for Healthcare

CASE STUDY: SWIFTLY RESOLVING A SECURITY CRISIS

How Weilheim-Schongau fended off a malware attack with Microsoft Defender for Endpoint

Even small organizations can suffer devastating security threats. For Weilheim-Schongau, a hospital system nestled in Upper Bavaria, the crisis began when an employee unwittingly opened an unfamiliar email attachment that turned out to be a crypto-trojan. Weilheim-Schongau was subsequently attacked by notorious ransomware GandCrab 5.3, which started to inflict extreme and rapid privacy breaches, accompanied by a ransom demand for Bitcoin.

While isolated, Weilheim-Schongau was not alone. It had the right people and the right tools in place. The organization alerted a Microsoft Gold Partner, cybersecurity firm sepago, which knew what step one was: Microsoft Defender for Endpoint.

"The first step was to onboard to Microsoft Defender to stop the malware from spreading further," says Alexander Benoit, Lead Security Analyst at sepago.

Within 72 hours, the crisis was averted. Because of the hospital system's strong emergency preparation plan, paired with the right partnerships, there was no interruption in care.

Learn more about how Weilheim-Schongau successfully defended its data

> Our patients never noticed a thing. Thanks to Microsoft Defender, we incurred no damage or lost data.
>
> **Florian Diebel**
> Managing Director, Weilheim-Schongau Hospital

Secure your data and network

Prevent data breaches and cyberattacks on both desktop and mobile devices

Health organizations are increasingly vulnerable to data breaches and cyberattacks. Healthcare organizations are at risk from phishing. Medical apps and mobile devices also introduce risk. A chief source of breaches is not having the right protective technology in place. But what questions do you need to ask to ensure that you choose the right cloud solution? Use this upcoming section to ensure that your healthcare organization undergoes digital transformation smoothly and safely.

What should your strategy be?

Healthcare organizations have a powerful responsibility as 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 policies and data access.

Start with these questions

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

Do you have trusted partners that help you meet your HIPAA compliance goals?

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're remote or traveling?

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

Secure your data and network

How can it help your organization?

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, assuring patients their sensitive information remains secure. Our built-in tools monitor health apps and data sets to prevent malicious access and detect and respond to cyberthreats faster.

Key benefits

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

- **Minimize** risk while sharing and integrating patient data securely across different medical systems.
- **Boost** security and privacy.
- **Minimize** 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.

CASE STUDY: PIVOTING TO A REMOTE WORKFORCE

How Ashford and St. Peter's Hospitals National Health Service Foundation Trust pivoted swiftly to a virtual work environment without compromising security

When a global health crisis struck, United Kingdom–based Ashford and St. Peter's Hospitals were able to pivot smoothly to a remote workforce model by incorporating Windows Virtual Desktop. By leveraging technology, the hospitals avoided the cost and logistical burden of shipping out new equipment to 350 employees.

Automating security for greater peace of mind was one of the deciding factors for choosing a Microsoft solution. With less manual work, the organization can focus on providing the best patient care in a secure environment.

With Windows Virtual Desktop, it's all done for us in the cloud. Devices automatically get the latest and greatest updates, and we don't have to worry about it. Before, we were patching computers daily.

Morné Beck
Head of IT,
Ashford and St. Peter's Hospitals National Health Service Foundation Trust

Learn how Ashford and St. Peter's Hospitals National Health Service Foundation Trust maintains high security standards

Conditional access

Ensure that only the right people have access to the right information at the right time

What should your strategy be?

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

- **Permit and restrict data access** based on the device risk level to limit the 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.

Start with these questions

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

Can you control access to your data across all PCs, tablets, and smartphones used by the people inside and outside your organization—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?

Conditional access

How can it help your organization?

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

No matter where data is—on a local server, in the public cloud, or on portable devices—Microsoft helps you ensure that those accessing your network are who they say they are, that their access to data is controlled, and that only those who are authorized to view protected health information can do so.

Key benefits

Transforming helps you:

- **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 data loss.
- **Establish** standard security best practices and industry compliance.

CASE STUDY: CREATING A SECURE REMOTE WORKFORCE

How Premera leveraged Microsoft 365 to swiftly create a secure remote workforce

When an unprecedented health crisis dictated an urgent shift in its workforce, Premera Blue Cross, a leading health insurance company in the Pacific Northwest, had to implement its five-year mobile work plan a little sooner than intended.

Security was top of mind as the organization pivoted to a remote workforce. To enable secure remote work, IT used Conditional Access policies in Microsoft Azure Active Directory to create robust adaptive access policies for on-premises and cloud applications on employees' laptops and smart devices.

Premera also deployed Microsoft Intune to secure work files inside encrypted containers on employees' personal phones so that they could use their own devices for work while reducing the risk of leaking data.

When it comes to sensitive information on employees' Surface devices, device encryption enables Premera to protect data so it can only be accessed by authorized individuals. All Surface devices feature a Trusted Platform Module that makes it fast and easy to encrypt data. The company also takes advantage of Azure Advanced Threat Protection and Microsoft Defender Advanced Threat Protection.

See how Premera pivoted while still protecting data

> The next level for security is that single pane of glass for multiple points of threat intelligence. The threat intelligence gained from an Azure risk-based platform that looks for employees' credentials on the dark web will give us a much better picture of user behavior and improve our overall security posture.
>
> **Dennis Armstrong**
> Enterprise Messaging Engineer,
> Premera Blue Cross

04
Addressing compliance challenges

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

Meeting compliance obligations in a dynamic regulatory environment is complex. Many health organizations need to take inventory of their data protection risks to manage the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

How can healthcare providers be sure that a solution is trustworthy?

Certifying a solution's reliability is crucial. Ensuring personal information privacy isn't just a moral issue, but a legal one too. You'll want to ensure that all patient and organizational 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 with securing infrastructure and patient information? Here's some actionable information to get you started.

> We look at compliance as people, process, and technology. You have to have all three in order to be compliant.[5]

Nancy Wilson
Vice President of Privacy and Compliance, Lumen21

Microsoft Cloud for Healthcare helps support your needs to meet your compliance requirements in a dynamic environment.

Get help meeting compliance standards with Microsoft Cloud for Healthcare

Assess the risks

Get support ensuring your compliance standards are met, guard against security threats, and protect personal data

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.

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 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?

Assess the risks

How can it help your organization?

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—instead of slowing things down—by adding these layers of protection. Stay ahead of all your tasks so that you can assign responsibilities to the right employee. Plus, by strengthening your process accountability, you'll further ensure compliance.

Key benefits

Transforming helps you:

- **Access** advanced compliance-related resources to ensure best practices.
- **Control** access to sensitive data with advanced threat protection: identity verification and multiple encryption methods.
- **Receive** actionable intelligence with advanced e-discovery.
- **Classify, protect, and govern** sensitive information automatically.
- **Prevent** malicious or inadvertent data loss or exposure.
- **Provide** transparency by controlling how consumer data is accessed.

CASE STUDY: ENABLING A CENTRALIZED VIEW OF DATA

How Arkin transitioned to the cloud securely with Microsoft 365

To ensure that its transition to a cloud workplace would not compromise the safety of its information, Arkin, one of the largest mental health networks in the Netherlands, turned to Microsoft 365 security and compliance solutions. Before a global health crisis struck, Arkin's IT staff enabled modern cloud management with Microsoft Enterprise Mobility + Security. "Going to the cloud, we wanted to work anyplace, anytime, and anywhere without compromising privacy," says Fred Pietersma, Chief Information Security Officer at Arkin. "Microsoft 365 has the security tools to enable that avant-garde way of working."

Arkin began its transition to a remote workforce by deploying Microsoft Office 365 Advanced Threat Protection and Microsoft Azure Advanced Threat Protection so its IT teams could monitor a single portal for alerts. Each team used to operate independently. Today, IT employees in infrastructure, engineering, and Office 365 have a holistic view of the entire cloud environment.

Learn more about how Microsoft 365 keeps Arkin secure

> Now we have a single dashboard and we see the alerts in real time, so we work together to keep the environment safe. … This has been even more valuable since everyone is working remotely.
>
> **Fred Pietersma**
> Chief Information Security Officer, Arkin

Accountability and transparency

Create automated processes to ensure governance compliance and simplify audit trails

What should your strategy be?

Streamline your compliance and reporting business processes. Coupled with modern technologies like AI and machine learning, data can determine procedures—which extends to both clinical and operational 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, labeling, and encryption capabilities for enhanced protection across devices, apps, cloud services, and on-premises solutions.

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?

Accountability and transparency

How can it help your organization?

With a streamlined approach, you'll increase transparency and control data flow for both personalized 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 effort required for discovery.

Key benefits

Transforming helps you:

- **Adhere** to corporate data governance policies.
- **Automate** remediation and investigation to reduce the burden on your team.
- **Gather** improved insights about health operations.
- **Manage and monitor** your processes in real time.

05
Choosing a cloud service provider

Maintain data reliability to support business continuity

Safeguard against service interruptions, from natural disasters to malware attacks

What should your strategy be?

A disruption to infrastructure services and your mission-critical business apps can put patients' lives at risk and reduce revenue and productivity. But don't worry—you can address this risk with built-in 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 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 integrate into your organization's current and future operations?

Maintain data reliability to support business continuity

How can it help your organization?

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 to make data-driven decisions. Plus, you can protect operational services in the event of a service disruption.

Key benefits

Transforming helps you:

- **Maintain** business continuity with data resiliency.
- **Avoid** an unexpected disruption.
- **Eliminate** data risks while ensuring data integrity and availability.
- **Comply** with industry standards.

CASE STUDY: BUSINESS CONTINUITY IN ACTION

How the Canadian Mental Health Association used Microsoft 365 to serve clients continuously during an unexpected crisis

When a global health crisis struck, the Canadian Mental Health Association Peel Dufferin branch (CMHA Peel Dufferin) knew that mental health patients would be needing its services more than ever. Despite the unexpected nature of the crisis, an interruption in service was not an option.

"We believed that it was crucial to support our community-based workforce's need to work remotely and securely," says Lawrence Swailes, Director of Innovation at CMHA Peel Dufferin.

To achieve that goal, the organization's IT team turned to Microsoft Azure solutions and services. CMHA Peel Dufferin secured the organization's infrastructure in the cloud with Azure and deployed Microsoft 365 and Microsoft Teams.

> When our team had to quickly shift to a new model for supporting our clients in an accessible, low-cost way, we turned to Microsoft Teams. Given our concern over privacy on other platforms, it was an easy choice for a way to connect community support workers with clients.
>
> **Nivetha Sivaranjan**
> Community Support Worker,
> CMHA Peel Dufferin

See how CMHA Peel Dufferin pivoted swiftly and safely in a crisis

Trusted cloud healthcare principles

Security

Protecting you from cyberthreats

Enable anyone to work freely and securely from anywhere on any platform.

Privacy

Giving you control over access to your data set

Provide greater user control and transparency and extend compliance protections to customers worldwide.

Compliance

Unparalleled investment in meeting global standards

Focus efforts to comply with national, industry, and customer-specific compliance policies worldwide.

Trust

A set of foundational principles that guide business in the cloud

Leverage leading technologies and processes to deliver best-in-the-business capabilities.

Cloud technology is the way forward

Healthcare organizations must digitally transform to meet modern expectations and standards. Adopting cloud technology is what will make digital transformation doable.

Cloud technology enables organizations to:

- **Automate** manual tasks.
- **Modernize** outdated systems.
- **Create** a thriving infrastructure.
- **Empower** healthcare workers to focus on patient care.

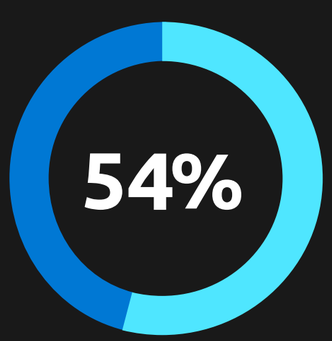
Lingering hesitations around security should not hold organizations back from making this essential shift. While patient confidentiality and compliance are paramount, the answer is to find a trusted cloud provider, not to avoid innovation altogether. By choosing a trusted partner like Microsoft Cloud for Healthcare, organizations can benefit from an end-to-end, industry-specific partner with minimized risk.

Choosing the right solution ensures that healthcare organizations will collaborate for better outcomes, streamline operations, and protect highly sensitive information. There is no longer a need to choose between innovation and security. Both are now possible.

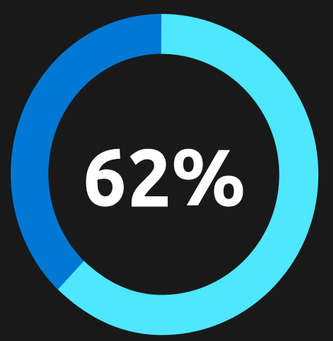
Microsoft Cloud for Healthcare empowers organizations to rise to the occasion in any circumstance, with benefits like:

- **Cost reduction** through consolidation of technologies.
- **Improved data agility** across disparate data sets for deeper, faster insights.
- **Accelerated machine learning** development for a less manual approach.
- **Increased data security** and secure sharing of patient information.

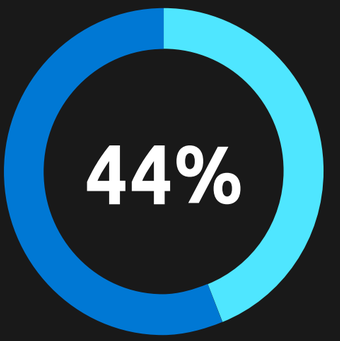
Harvard Business Review found that organizations that embrace data to drive transformations experience a:



growth in revenue and profits[6]



enhancement in customer satisfaction[6]



faster time to market relative to their peers[6]

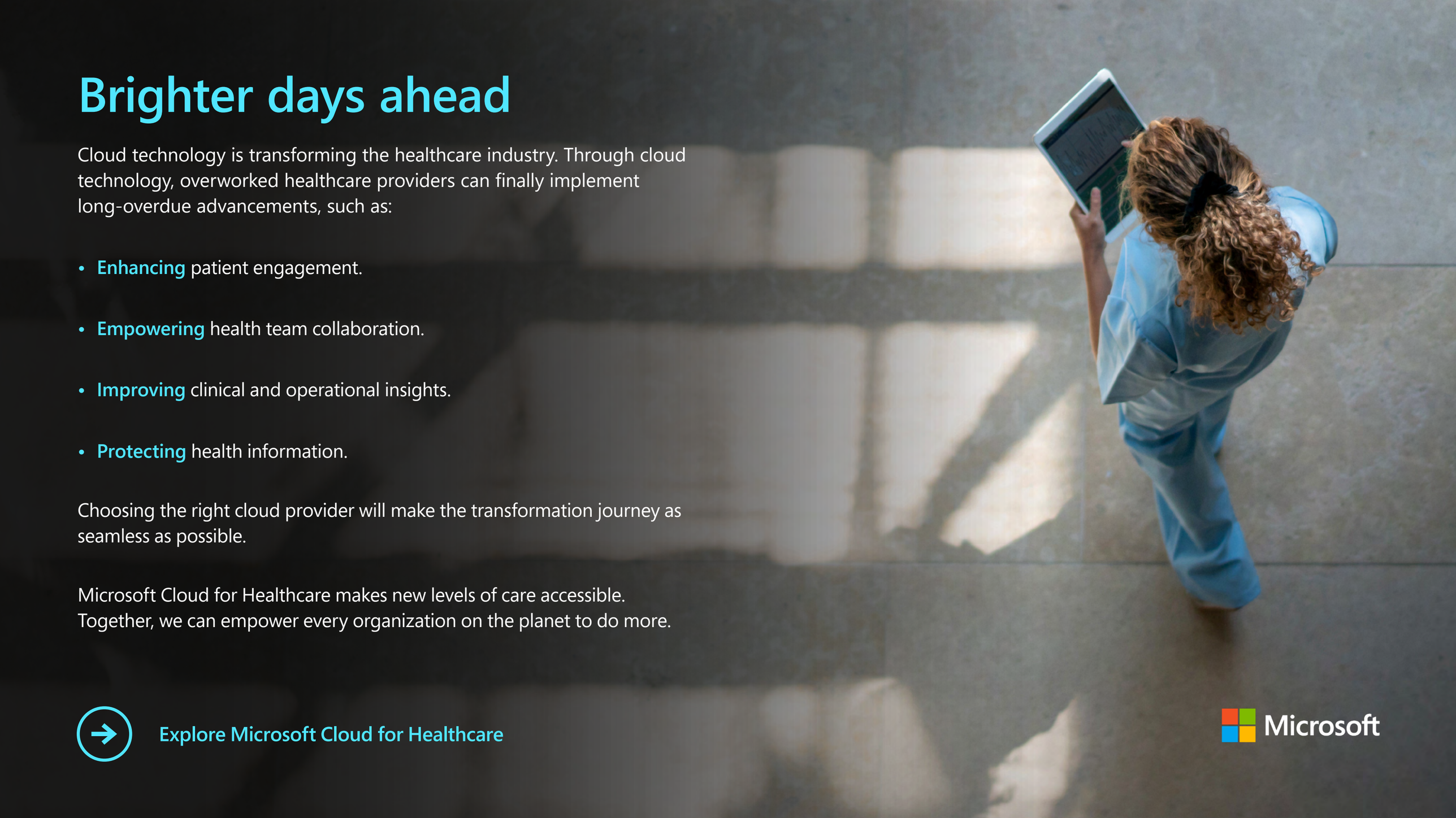
Brighter days ahead

Cloud technology is transforming the healthcare industry. Through cloud technology, overworked healthcare providers can finally implement long-overdue advancements, such as:

- **Enhancing** patient engagement.
- **Empowering** health team collaboration.
- **Improving** clinical and operational insights.
- **Protecting** health information.

Choosing the right cloud provider will make the transformation journey as seamless as possible.

Microsoft Cloud for Healthcare makes new levels of care accessible. Together, we can empower every organization on the planet to do more.



Explore Microsoft Cloud for Healthcare

Microsoft

Sources

[1] IBM Security and Ponemon Institute, *Cost of a Data Breach Report 2020*, 2020.

[2] IBM Security and Ponemon Institute, *Cost of a Data Breach Report 2019,* 2019.

[3] HIPAA One, sponsored by Microsoft, *HIPAA Compliance Microsoft Office 365 and Microsoft Teams*, April 2019.

[4] Black Book Market Research, "Attacks Predicted to Triple in 2021, Black Book State of the Healthcare Industry Cybersecurity Industry Report," November 13, 2020.

[5] Microsoft, Lumen21 customer success story.

[6] R "Ray" Wang, "How to Lead a Data-Driven Digital Transformation," *Harvard Business Review*, May 28, 2020.