CLEARDATA®

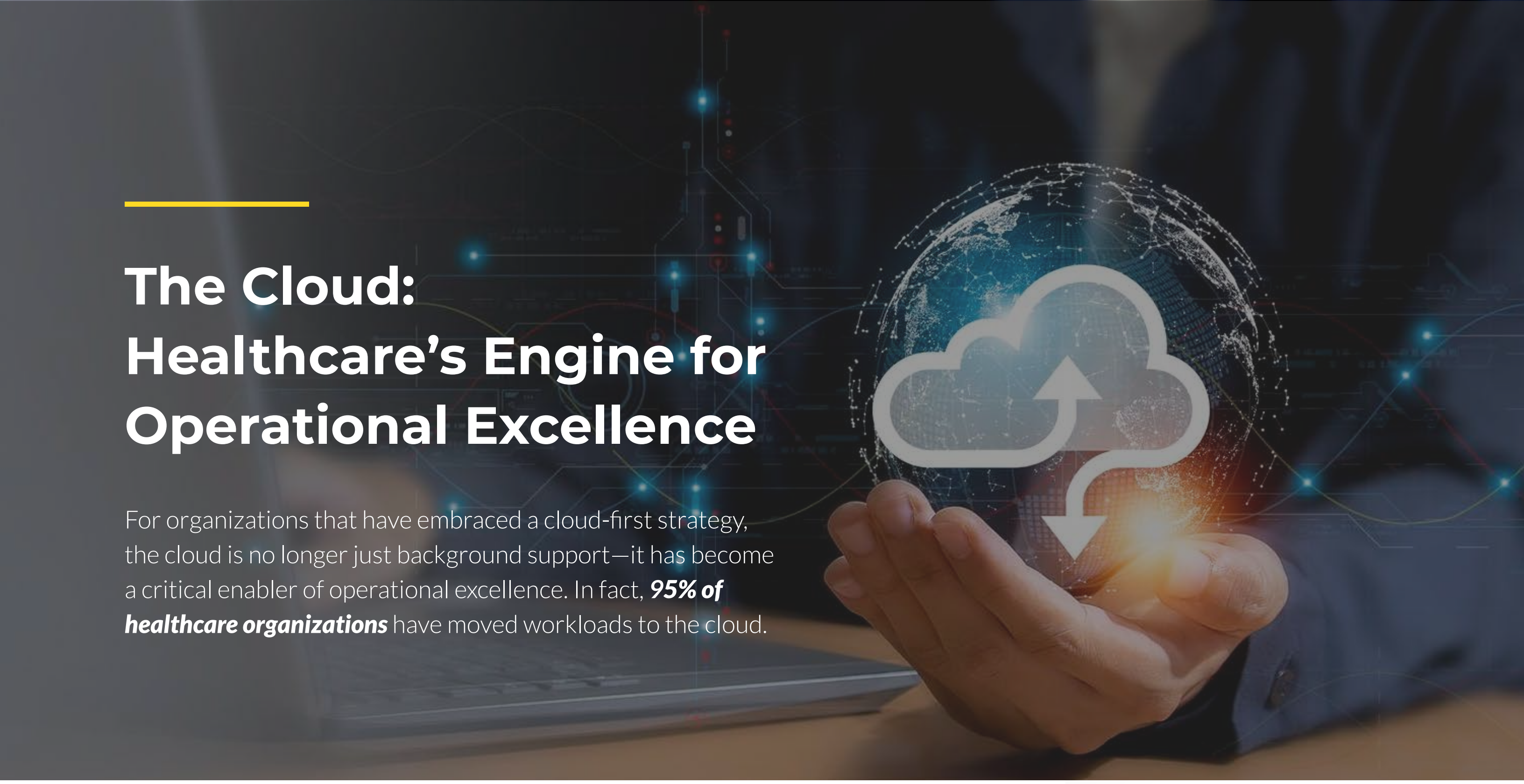
www.cleardata.com

Running Healthcare in the Cloud:

HOW TO BUILD SECURE, COMPLIANT, AND SCALABLE CLOUD OPERATIONS

A roadmap to protecting sensitive data by maximizing cloud operational excellence.

Table of Contents



The Cloud: Healthcare's Engine for Operational Excellence

For organizations that have embraced a cloud-first strategy, the cloud is no longer just background support—it has become a critical enabler of operational excellence. In fact, ***95% of healthcare organizations*** have moved workloads to the cloud.

Achieving operational excellence in the cloud requires a focus on three key pillars: ***security, compliance,*** and ***performance***. These foundational elements ensure healthcare organizations can maximize efficiencies while mitigating risks and meeting regulatory requirements. The following is an example of how healthcare platform ***Intelibly reaped the benefits*** of optimizing its cloud operations.

SECURITY: Protecting Healthcare Data in a Threat Landscape

Facing challenges in securing patient data from increasingly sophisticated cyber threats, Intelibly partnered with ClearDATA to build a secure and resilient cloud infrastructure.

By leveraging ClearDATA's CyberHealth™ Platform and managed services, Intelibly gained critical threat protection through Managed Detection & Response. The platform provided real-time threat intelligence, helping Intelibly mitigate risks and strengthen its overall security posture. This allowed them to scale operations with confidence, knowing that their data was safeguarded against evolving threats.

COMPLIANCE: Meeting Healthcare Regulations with Confidence

While the cloud offers flexibility and scalability, maintaining regulatory compliance remains a top concern for healthcare organizations. Currently, 74% of healthcare organizations still face compliance gaps that put patient data at risk. Intelibly faced similar challenges, struggling with time-intensive manual compliance processes that introduced inefficiencies and potential risks.

ClearDATA's compliance automation and continuous monitoring provided Intelibly with real-time visibility into their compliance status, ensuring adherence to HIPAA, NIST, and other regulatory frameworks. The result was a strengthened compliance posture, reduced operational burden, and the ability to onboard enterprise clients with stringent security and regulatory requirements.

PERFORMANCE: Driving Efficiency and Scalability in Healthcare Operations

Intelibly's transition to a well-architected cloud environment not only optimized their existing infrastructure but also provided scalability to support their rapid growth.

Through ClearDATA's AWS Well-Architected Framework Review (WAFR), Intelibly validated the efficiency of their cloud setup. The review confirmed that their cloud infrastructure was optimized for high performance, allowing them to scale rapidly without compromising reliability. Since implementing ClearDATA's services, Intelibly has nearly doubled its SMB customer base and is on track to onboard 40,000 additional accounts in Q1 2025.

Operational excellence isn't only a necessity for Intelibly. It will be essential for various organizations within the healthcare sector to bolster their cloud operations, including:

01 HealthTech ▶

As cloud-native organizations selling to large healthcare providers with strict security and compliance requirements, managing the cloud isn't HealthTech's core business. Instead, they face the burden of maintaining a secure, compliant infrastructure, which diverts resources away from improving products and services. A resilient cloud—secure, compliant, cost-efficient, and operationally streamlined—can empower HealthTech firms to focus on their mission: delivering cutting-edge solutions and improving patient outcomes, without compromising speed or innovation.

02 Payers ▶

Unlike legacy on-premise infrastructure, the cloud processes real-time data at scale, streamlining claims management to reduce errors and accelerate reimbursements while keeping operational costs in check.

Additionally, the cloud enables true innovation with advanced analytics and data interoperability, providing deeper insights into patient needs. This paves the way for personalized healthcare services that weren't feasible with outdated on-prem systems. By leveraging a secure, compliant, and scalable cloud, payers can overcome legacy limitations, drive sustainable growth, and improve member outcomes.

03 Providers ▶

By leveraging connected medical devices and optimizing processes, providers can focus on delivering quality care rather than managing tedious tasks. This approach supports efficient resource allocation, minimizes delays, and enhances outcomes in value-based care models. Through the effective use of technology and data, providers can make informed decisions and deliver responsive, patient-centered care.

04 Life Sciences ▶

By driving operational excellence, a resilient cloud accelerates speed-to-market by shortening testing cycles, enabling more tests to be conducted in less time. This increased testing capacity enhances the likelihood of bringing more groundbreaking treatments to market. With the right cloud infrastructure, life sciences organizations can innovate faster, reduce risks, and advance patient care while meeting the demanding requirements of the healthcare industry.

The Future of Healthcare in the Cloud

By 2027, 85% of healthcare applications will integrate AI-driven security—yet only 20% of organizations have AI-based cloud compliance monitoring today. Here's how you can get ahead of the technological innovations impacting the healthcare cloud and your path toward operational excellence.

Edge Computing: A Game Changer Closer to Home

Edge computing is increasingly playing a pivotal role in influencing operational excellence in the cloud. With healthcare devices becoming more advanced and the expansion of the ***Internet of Medical Things (IoMT),*** the capability to process data near its source is set to radically transform healthcare systems. Here's how:

- Reduced Latency: Edge computing allows healthcare organizations to analyze data at its source. This proves vital for immediate diagnoses and interventions.
- Improved Reliability: Edge computing boosts operational efficiency by providing distributed processing, thus elevating the reliability standard.
- Better Remote Patient Monitoring: The availability of more 5G-powered connected devices leads to improved and frequent real-time patient health monitoring, key for managing chronic diseases.

What Does This Mean for Your Security and Compliance Strategy?

- Secure patient data at the edge to reduce risk exposure and protect against unauthorized access.
- Implement encryption and access controls for sensitive data processed on edge devices.
- Ensure regulatory compliance by applying continuous monitoring to edge infrastructure.
- Strengthen endpoint security to mitigate risks associated with distributed computing environments.

Robotic Process Automation (RPA): A Solution for Healthcare Burnout?

RPA has become a pivotal player in driving operational excellence in the cloud. The impact is substantial across several areas, including:

- Operational Efficiency Improvement: RPA cuts through administrative burdens. It repurpoes invaluable staff hours towards more critical, patient-focused roles by automating routine tasks such as data entry or ***pharmacovigilance***.
- Error Reduction: RPA significantly curtails the risk of human errors, potentially making a profound difference in patient outcomes.
- Scalability Enhancement: RPA empowers hospitals and clinics to effectively manage resource demands that continually ebb and flow.

What Does This Mean for Your Security and Compliance Strategy?

▶ Implement RPA with built-in compliance checks to ensure adherence to HIPAA and other healthcare regulations.

▶ Secure RPA bots with identity and access management (IAM) controls to prevent unauthorized access.

▶ Monitor and audit RPA processes to detect anomalies and ensure data integrity.

▶ Apply encryption and secure data handling practices to protect sensitive patient information processed by RPA systems.

The AI Buzz: What Does It Mean for Healthcare?

AI is revolutionizing operational excellence in the cloud, shaping the future of efficient and effective operations. It's astounding to witness how AI is taking cloud operations to new heights. Examples include:

- Patient Diagnosis: Healthcare is incorporating machine learning algorithms to analyze patient data, allowing for quick and accurate diagnosis.
- Personalized Care Plans: AI technology can help develop patient-specific care plans that take into account each individual's unique needs and conditions.
- Drug Development: AI is being used to discover new drugs and optimize current drug regimens, leading to more effective treatments and a higher success rate in clinical trials.
- Robotic Surgery: With robotic surgery becoming more commonplace, AI can be used to improve surgical precision and reduce human error.

What Does This Mean for Your Security and Compliance Strategy?

- Implement AI-driven security analytics to detect and respond to threats in real time.
- Use AI-powered automation to streamline compliance workflows and ensure continuous regulatory adherence.
- Protect patient data by enforcing strict access controls and leveraging AI for anomaly detection.
- Ensure transparency and ethical AI use by incorporating explainability and audit mechanisms into AI-driven healthcare systems.

Interoperability and Data-Driven Healthcare

One of the leading causes of operational excellence in the cloud is the emergence of interoperability and data-driven healthcare. Here are some of the benefits of healthcare interoperability:

- Interoperability makes patient records, diagnostic results, and treatment plans easily available to authorized personnel on shared cloud platforms, mitigating delays and reducing redundancies in care delivery.
- Interoperability improves claims processing by streamlining communication between payers and providers. This results in faster reimbursements, reduced administrative burdens, and improved efficiency.
- Cloud-enabled data sharing accelerates medical research by allowing institutions to collaborate on large datasets, leading to advancements in treatments and evidence-based practices.
- Interoperability coordinates healthcare treatment to individual patient needs, thereby improving safety and quality while fostering a more sustainable healthcare system.

What Does This Mean for Your Security and Compliance Strategy?

- Ensure data interoperability standards, such as HL7 and FHIR, are met to maintain compliance.
- Implement strong access controls and encryption to secure shared healthcare data.
- Monitor and audit data exchanges to detect anomalies and prevent breaches.
- Use cloud-based compliance tools to ensure continuous adherence to healthcare regulations.

Challenges & Solutions to Cloud Operational Excellence for Healthcare

PROBLEM 01: The Skills Gap Is Slowing Cloud Adoption

Cloud environments require specialized expertise that differs greatly from managing legacy systems. Many IT teams are still in the process of upskilling or adapting to cloud technologies, leaving organizations struggling to keep pace with rapidly evolving demands.

Key areas where skills gaps commonly arise include:

- **Transitioning from Legacy to Cloud:** Moving from on-premise systems to cloud infrastructure involves complex migration strategies, rearchitecting applications, and integrating modern cloud-native solutions.
- **Navigating the Threat Landscape:** Cyber threats targeting healthcare are increasingly sophisticated. Staying ahead requires continuous monitoring, threat hunting, and advanced security practices, which can strain teams without cybersecurity expertise.
- **Harnessing Cloud Innovations:** Keeping up with fast-evolving cloud capabilities—such as AI, automation, and multi-cloud strategies—requires a deep understanding of cloud services to unlock their full potential.
- **Maintaining Continuous Compliance:** Meeting strict regulatory requirements (HIPAA, HITRUST, GDPR) in dynamic cloud environments demands constant attention to compliance policies and security practices.

SOLUTION: Build a Future-Ready Cloud Team

- Invest in cloud training programs for IT and security teams to strengthen cloud expertise.
- Leverage managed cloud security services to supplement internal skill gaps and enhance cloud security posture.
- Automate compliance management to reduce the burden on IT teams and maintain regulatory standards.
- Implement threat intelligence and monitoring solutions to proactively detect and mitigate risks.
- Develop a cloud governance framework that ensures best practices for security, compliance, and performance.

PROBLEM 02: Compliance Risks Are Rising in Dynamic Cloud Environments

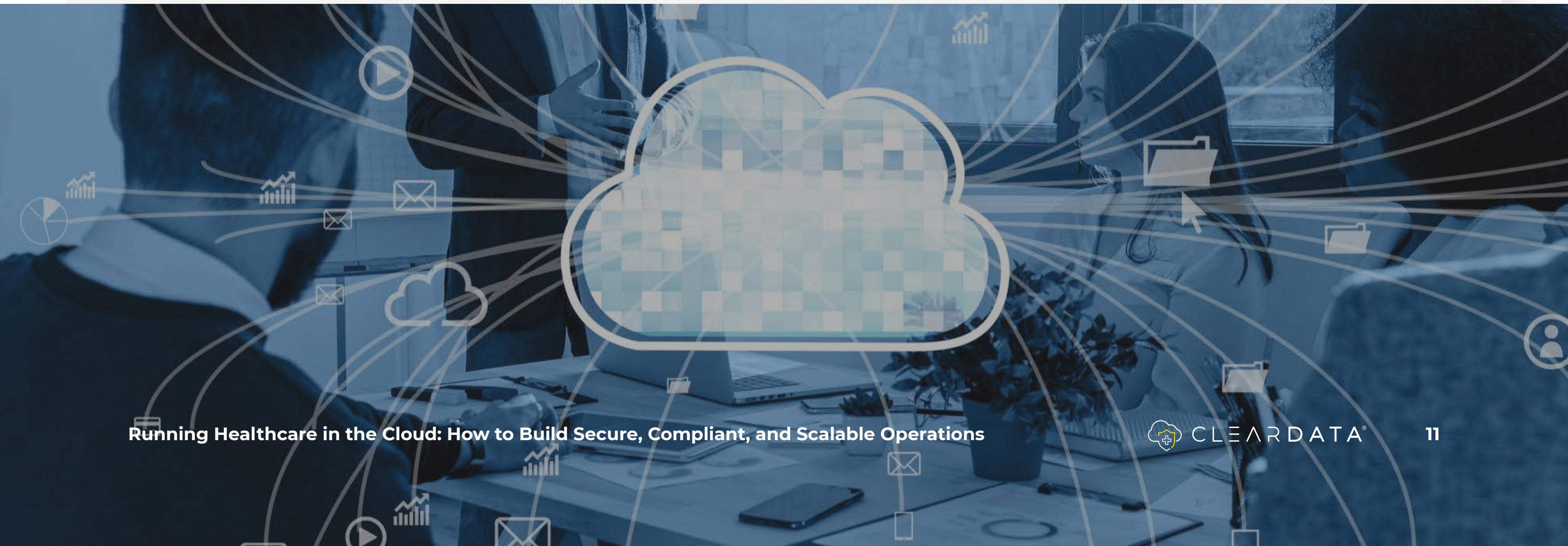
Healthcare organizations operate in one of the most heavily regulated industries, with strict requirements around data security, privacy, and operational processes. In cloud environments, maintaining continuous compliance with regulations like HIPAA, HITRUST, and GDPR is far more complex than in traditional on-premise systems.

Unlike legacy infrastructure, where environments are relatively static, the cloud is dynamic—constantly evolving with new services, configurations, and integrations. This introduces unique challenges, such as:

- **Increased Complexity:** Managing compliance across multi-cloud environments or hybrid architectures adds layers of complexity, requiring real-time monitoring and continuous auditing to stay compliant.
- **Shared Responsibility Model:** Cloud providers offer infrastructure security, but healthcare organizations remain responsible for data protection and compliance.
- **Slower Innovation Cycles:** Teams are forced to move cautiously, knowing that the risk of non-compliance could result in heavy fines, reputational damage, and loss of patient trust.

SOLUTION: Strengthen Compliance with Cloud-First Security Measures

- Deploy cloud security posture management (CSPM) tools to automate compliance monitoring and policy enforcement.
- Implement real-time auditing and continuous compliance checks across cloud workloads.
- Establish clear governance frameworks to define security and compliance responsibilities within the shared responsibility model.
- Use encryption and access controls to safeguard sensitive healthcare data in multi-cloud environments.
- Conduct regular compliance assessments to ensure adherence to evolving regulatory standards.



PROBLEM 03: Cloud Security Risks Are More Sophisticated Than Ever

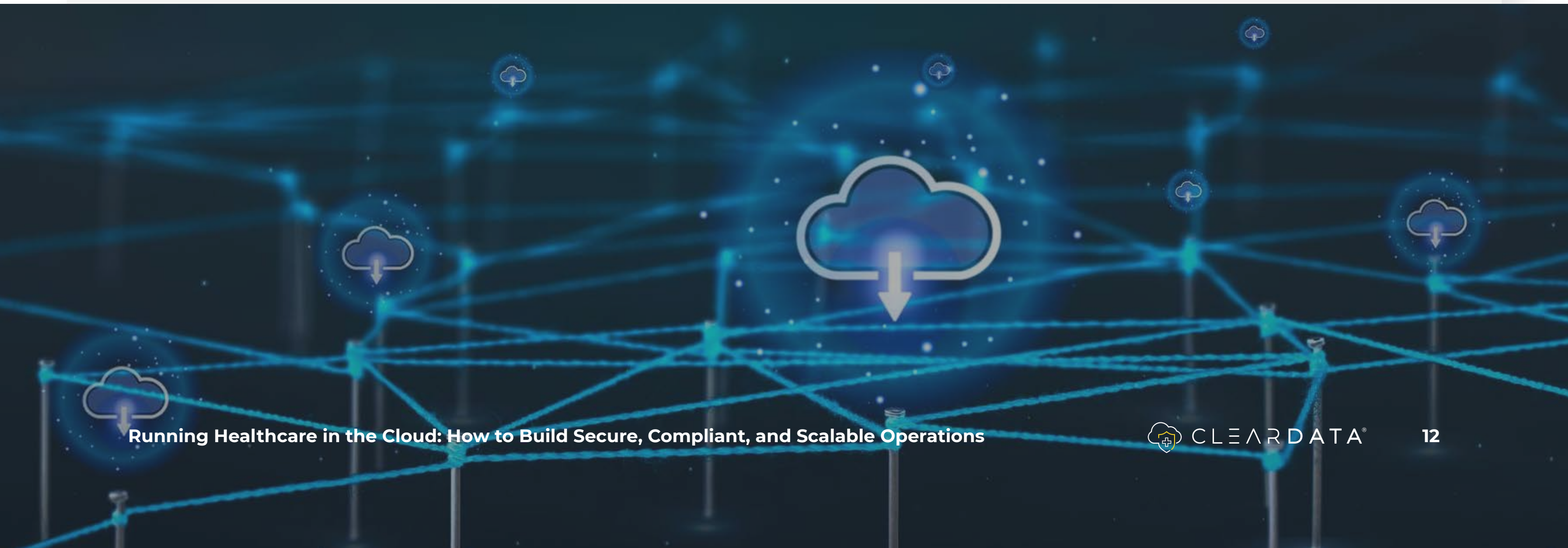
Cyber threats are more sophisticated and frequent in cloud environments compared to legacy infrastructure, where security perimeters are easier to define and control. In the cloud, the attack surface is broader, requiring new security strategies to protect sensitive patient data.

Security challenges in the cloud include:

- **Broader Attack Surface:** Cloud environments have more entry points, making them a prime target for cybercriminals seeking access to valuable patient records.
- **Dynamic Environments:** What's secure today may not be tomorrow due to changes in configurations or new threats.
- **Compliance and Security Overlap:** Keeping compliance and security intact adds significant complexity, especially when adopting cloud innovations or multi-cloud strategies.
- **Shared Responsibility:** While cloud service providers manage infrastructure security, organizations are responsible for securing their applications, data, and configurations—a responsibility many healthcare organizations are still adapting to.

SOLUTION: Strengthen Cloud Security with Proactive Risk Management

- Implement a zero-trust security model to enforce least privilege access and minimize risk.
- Deploy real-time threat detection and response solutions to identify and mitigate security incidents.
- Use automated security posture management tools to continuously monitor for misconfigurations and vulnerabilities.
- Encrypt sensitive patient data at rest and in transit to ensure end-to-end protection.
- Conduct regular penetration testing and security audits to proactively identify weaknesses in cloud environments.
- Educate staff on cloud security best practices to minimize human error and insider threats.



HEALTHTECH'S BIGGEST CHALLENGE:

Balancing Innovation with Security and Compliance

As cloud-native organizations, HealthTech companies face unique challenges in scaling their innovative applications. The primary hurdles aren't just financial but also operational and strategic:

Security and Compliance Strain Resources:
Operating securely in the cloud while meeting compliance standards often diverts resources away from growth acceleration. Many companies also lack the specialized talent to keep up with ever-evolving security and compliance demands.

Inefficient Security Practices:
Without a security-by-design approach like DevSecOps, workloads can be vulnerable. This leads to costly remediation efforts in production, slowing down innovation and increasing risks.

Technical Debt from Growth:
The rapid adoption of new technologies like AI can create inefficiencies in architecture, compounding risks around security, compliance, and cost management.

Solution: Align Innovation with Security and Compliance from the Start

✓ Adopt a DevSecOps approach to integrate security and compliance early in the development lifecycle.

✓ Leverage managed cloud security services to reduce the burden of in-house compliance management.

✓ Implement automated security and compliance monitoring to detect vulnerabilities before they become risks.

✓ Develop a scalable cloud architecture that supports growth while maintaining security best practices.

✓ Conduct regular security audits and compliance assessments to stay ahead of regulatory changes.

PAYER'S BIGGEST CHALLENGE:

Fragmented Systems That Hinder Interoperability

Drawing insights from various sources, here are some common challenges healthcare payers make during their digital transformation:

Fragmentation and Inconsistency:
Having too many sources of truth and allowing technical taxonomies to proliferate without consolidation can create confusion and inefficiency, undermining the transformation process.

Relying on Outdated Technology:
Despite the availability of advanced digital health technologies, some continue to rely on outdated systems and approaches, limiting their ability to innovate and respond to market demands.

Lack of Interoperability:
Less interoperability means fewer efficient, patient-centric services. When systems cannot seamlessly exchange data, it leads to delays, inaccuracies, and redundancies that negatively impact decision-making and overall operational efficiency.

Solution: Build a Unified and Interoperable Digital Infrastructure

✓ Standardize data models and taxonomies to ensure consistency across systems.

✓ Invest in modern API-driven architectures to facilitate seamless data exchange.

✓ Leverage cloud-based interoperability solutions to unify disparate systems and improve data accessibility.

✓ Phase out outdated technology and transition to scalable, compliant cloud platforms.

✓ Implement real-time data validation and integration frameworks to enhance operational efficiency.

PROVIDER'S BIGGEST CHALLENGE:

Underutilization of Compliance Automation

Just like payers, providers also make mistakes when digitally transforming their operations. This includes failing to address interoperability between different healthcare systems and allowing equal access to digital services. This can limit the reach and impact of digital transformation efforts.

If providers rely on manual processes, they are prone to errors, inconsistencies, and delays. This not only increases administrative workloads but also distracts staff from patient care, undermining the overall quality of service delivery.

A lack of automated compliance systems can inhibit adaptation to regulatory updates, which could result in further misalignments and non-compliance risks. On a broader scale, it reduces the organization's capacity to streamline operations, optimize resource allocation, and foster trust across stakeholders, including patients.

Solution: Implement Compliance Automation to Improve Efficiency and Accuracy

✓ Deploy automated compliance management tools to ensure continuous adherence to HIPAA, HITRUST, and other healthcare regulations.

✓ Integrate interoperability solutions that enable seamless data exchange between different healthcare systems.

✓ Leverage AI-driven automation to reduce administrative workloads and improve operational efficiency.

✓ Establish real-time compliance monitoring to proactively identify and address regulatory risks.

✓ Train staff on best practices for compliance automation to enhance adoption and optimize usage.

LIFE SCIENCE BIGGEST CHALLENGE:

Over-Reliance on Manual Data Handling

The life sciences segment continues to depend heavily on manual data handling processes, which inevitably increase the likelihood of errors, inefficiencies, and inconsistencies. This approach jeopardizes data accuracy and hampers decision-making and overall operational efficiency. Automating data collection and analysis processes is critical to minimizing these risks and ensuring reliable outcomes in research and development initiatives.

Solution: Automate Data Handling to Improve Accuracy and Efficiency

Implement AI-driven data analytics to streamline research and development processes.

Automate data collection and validation to reduce human errors and improve accuracy.

Leverage cloud-based data management platforms to enhance accessibility and collaboration.

Integrate automated compliance checks to ensure regulatory adherence in data handling.

Train research teams on best practices for using automation tools to optimize efficiency.

Building Operational Excellence Through Compliance

How Does Noncompliance Affect Operational Excellence?

Noncompliance costs healthcare organizations an average of $9.2 million per incident. That leads to compliance debt, which negatively impacts operational excellence because compliance is the backbone of operational integrity and financial health in healthcare technology.

What Is Compliance Debt?

Compliance debt is the accumulation of unresolved compliance tasks, including technical, security, operational, and personnel requirements necessary for maintaining compliance.

Compliance debt results from choosing immediate convenience over long-term efficiency and security. Below are the different types of compliance debt that weaken an organization's compliance posture:

Technical Debt

The compromise between quick fixes and the future maintainability of healthcare systems.

Security Debt

Arising from inadequate security protocols which, if ignored, open the door to breaches and data theft.

Operational Debt

The inefficiencies and outdated processes that slow down compliance efforts.

Personnel Debt

The gap in skills or knowledge within the team, hindering the ability to maintain or enhance the compliance environment.

Step-By-Step Strategies for Reducing Compliance Debt

Mitigating compliance debt and enhancing operational excellence requires strategic planning and proactivity. Here are some strategies you should implement if you're facing compliance debt:

1. Identify Gaps in HIPAA, HITRUST, and GDPR
2. Invest in robust IT governance
3. Enhance cyber defense mechanisms
4. Build a skilled workforce
5. Identify areas of risk and opportunity
6. Make compliance an integral part of the organizational culture and operational strategy
7. Utilize technologies and frameworks that automate compliance tasks
8. Engage in regular compliance and security training
9. Conduct periodic assessments for security and compliance architecture
10. Implement AI-driven policy enforcement tools.
11. Provide security training for engineering teams

Best Practices from Leading Healthcare Organizations

Automate Compliance Monitoring

Top-performing healthcare providers integrate AI-powered compliance monitoring tools to detect vulnerabilities in real time, reducing risk exposure.

Continuous Compliance Assessments

Industry leaders conduct quarterly security and compliance audits to stay ahead of regulatory changes and mitigate risks proactively.

Zero-Trust Security Model

Many healthcare organizations adopt a zero-trust approach, ensuring that all users and devices are authenticated and continuously verified.

Ongoing Staff Training

Regular compliance and security training programs are mandatory for all employees, ensuring awareness and reducing human error.

Data Encryption and Access Control

Enforcing strict encryption and role-based access policies limits unauthorized access and enhances patient data protection.

Proactive Threat Management: Securing Your Healthcare Cloud for Operational Excellence

5 Critical Threats CISOs Must Prioritize in 2025 & Beyond

1. A typical healthcare record has ***42 million sensitive data records***
2. A single ***PHI record can fetch as much as $250 for a hacker***, making it 10X more valuable than credit card data
3. ***50% of organizations use a significant part of their IT budgets for cybersecurity, highlighting the growing cost of securing sensitive data***
4. ***92% of respondents said their cybersecurity budget is growing year over year***, reflecting the urgency of defense strategies
5. Cloud security gaps cannot be overlooked, with 19% of organizations reportedly prioritizing cloud infrastructure to safeguard against cyber threats

In short, cybersecurity in healthcare is more important than ever. It's the only way to defend from the threat of cyberattacks that prevent operational excellence.

But how?

The Role of Proactive Threat Management

Proactive threat management involves building multiple layers of defense that reduce risks before they escalate into serious threats. By combining Cloud Security Posture Management (CSPM) with managed detection and response (MDR), organizations can create a more resilient security strategy.

Cloud Security Posture Management: The First Line of Defense

CSPM is essential for maintaining elevated compliance levels and minimizing the cloud's attack surface. By continuously monitoring cloud environments for vulnerabilities and misconfigurations, CSPM helps healthcare organizations proactively prevent breaches before they occur.

Threat Intelligence and Proactive Threat Hunting

Effective cybersecurity requires more than monitoring—it demands proactive threat hunting and intelligence gathering. By staying ahead of emerging threats, healthcare organizations can detect indicators of attack and compromise before damage is done.

- Threat Intelligence Tracking: Monitor evolving attack patterns and emerging vulnerabilities to strengthen your defense strategy.
- Proactive Threat Hunts: Actively search for hidden threats in your cloud environment, identifying suspicious behavior that automated systems might miss.
- Mitigation and Containment: When indicators of compromise are found, swift action can prevent escalation and protect patient data.

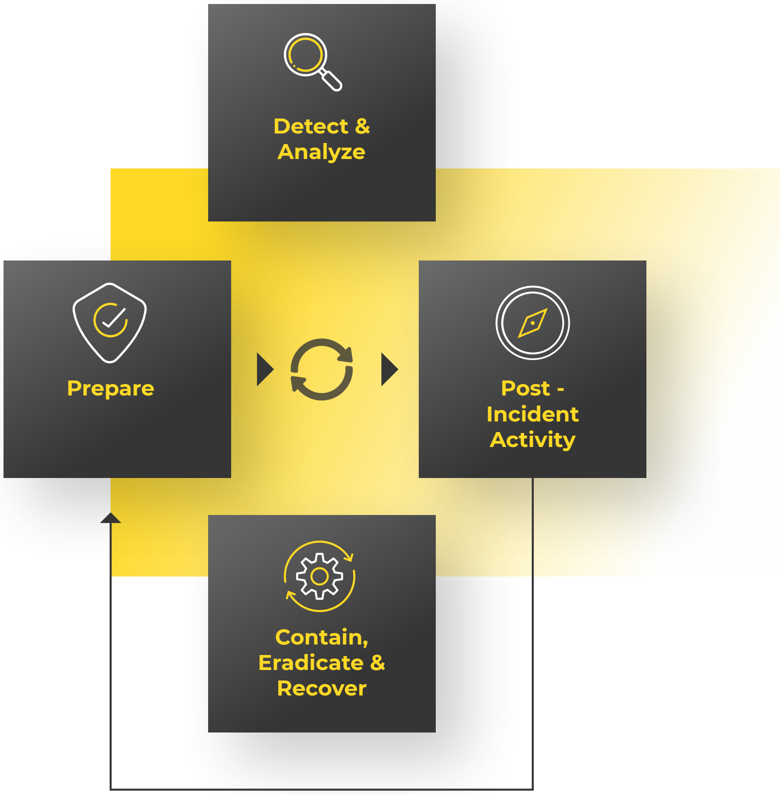
MDR's Role in Active Defense

MDR provides a dedicated team to oversee your organization's digital security, constantly monitoring and addressing cyber threats.

By offering 24/7 cloud monitoring, successful MDR experts act as your cyber threat hunters, diligently detecting and handling potential risks to your organization and its sensitive data.

Benefits of an MDR Service

- **Preventing Cyberattacks:** Using MDR services, healthcare organizations can avoid the crippling costs and disruption of cyberattacks. They provide a ***swift and efficient response to threats***, preventing data breaches, financial losses, and damage to your reputation.
- **Resource Optimization:** By leveraging MDR services, healthcare providers can free up valuable IT resources, allowing their teams to focus on what truly matters—patient safety, innovation, and business growth.



The Importance of Proactive Threat Hunting in Healthcare Cybersecurity

The importance of proactive threat hunting can't be overstated. Traditional security models focus on responding to breaches, but ***ClearDATA*** sees cybersecurity as a continuous, preemptive effort to reduce risk before an attack occurs.

By elevating compliance levels through Cloud Security Posture Management (CSPM), healthcare organizations can minimize their attack surface, reducing the number of exploitable entry points. Proactively remediating vulnerabilities and misconfigurations ensures fewer opportunities for exploitation, strengthening security from the inside out. Meanwhile, tracking real-time threat intelligence and conducting ongoing threat hunts allows organizations to detect early indicators of attack and compromise, rather than reacting after the damage is already done.

In short, proactive threat hunting shifts cybersecurity from a recover-from-cyber-threats mindset to actively staying ahead of them.

Building a Resilient Cloud Infrastructure for Operational Excellence

Proactive Elements

A resilient cloud infrastructure must withstand attacks and adapt to a changing environment to proactively address risks before they become critical.

To achieve this level of resilience, healthcare organizations should focus on:

- ▶ Proactive Risk Management and Access Hygiene: Good access hygiene and consistent security practices give authorized users the right level of access at the right time.
- ▶ Managing Technical Debt: Modernizing outdated systems, unpatched software, and legacy infrastructure to limit risk exposure.
- ▶ Planning for Adaptability and Future Growth: This includes implementing cloud-native architecture, scenario planning, and continuous improvement.

Response Elements

To build a truly resilient infrastructure that supports operational excellence, healthcare organizations must prioritize:

- ▶ Disaster Recovery Planning: A well-crafted disaster recovery plan reduces downtime and facilitates rapid restoration of critical services, minimizing the impact on patient care.
- ▶ Multi-Cloud Strategies: Distributing workloads across multiple cloud environments reduces dependency on a single provider.
- ▶ Incident Response Protocols: Outlining clear roles, responsibilities, and actions to take during an incident enables a swift and coordinated response.

How Enhanced Cybersecurity Improves Operational Outcomes in the Cloud

Implementing robust cybersecurity practices directly contributes to reduced downtime, improved trust, and a stronger security posture within healthcare operations.

- ▶ By proactively addressing vulnerabilities and deploying advanced threat detection systems, organizations significantly minimize the risk of disruptions caused by cyberattacks.
- ▶ Robust cybersecurity measures foster trust among patients and stakeholders. PHI remains secure, reinforcing confidence in the provider's ability to safeguard sensitive data.
- ▶ Consistent and well-defined cybersecurity strategies enhance an organization's overall security posture. Regular vulnerability assessments, employee training programs, and a commitment to implementing the latest security technologies create a resilient digital environment capable of adapting to evolving threats.

The CISO's Playbook for Threat Prevention:

The CISO's Playbook for Threat Prevention:

- Adopt CSPM & MDR solutions for real-time cloud security monitoring
- Conduct quarterly attack simulations to test incident response readiness
- Implement cloud IAM best practices (least privilege, MFA, zero-trust)
- Regularly update and patch all systems to mitigate known vulnerabilities
- Deploy endpoint detection and response (EDR) tools to enhance endpoint security
- Establish a continuous security awareness training program for employees
- Develop a risk-based vulnerability management strategy to prioritize critical threats
- Conduct third-party risk assessments to ensure vendor security compliance
- Enforce network segmentation to limit lateral movement in case of a breach
- Utilize encryption for data at rest and in transit to protect sensitive patient information
- Integrate AI-driven threat intelligence platforms to detect emerging threats proactively
- Maintain a robust data backup and recovery strategy to minimize the impact of ransomware attacks
- Implement real-time log analysis and SIEM solutions for enhanced visibility
- Continuously refine and test incident response and disaster recovery plans
- Develop a cloud governance framework to align security, compliance, and business objectives

30-60-90 Day Plan for Cloud Security & Compliance Maturity

Day 1-30: Assess Your Current State

- ✓ Conduct a comprehensive cloud security and compliance assessment
- ✓ Evaluate key areas: Compliance, security, and operational efficiency
- ✓ Establish a baseline for optimization and resilience

Day 31-60: Craft a Comprehensive Cloud Strategy & Optimize Resources

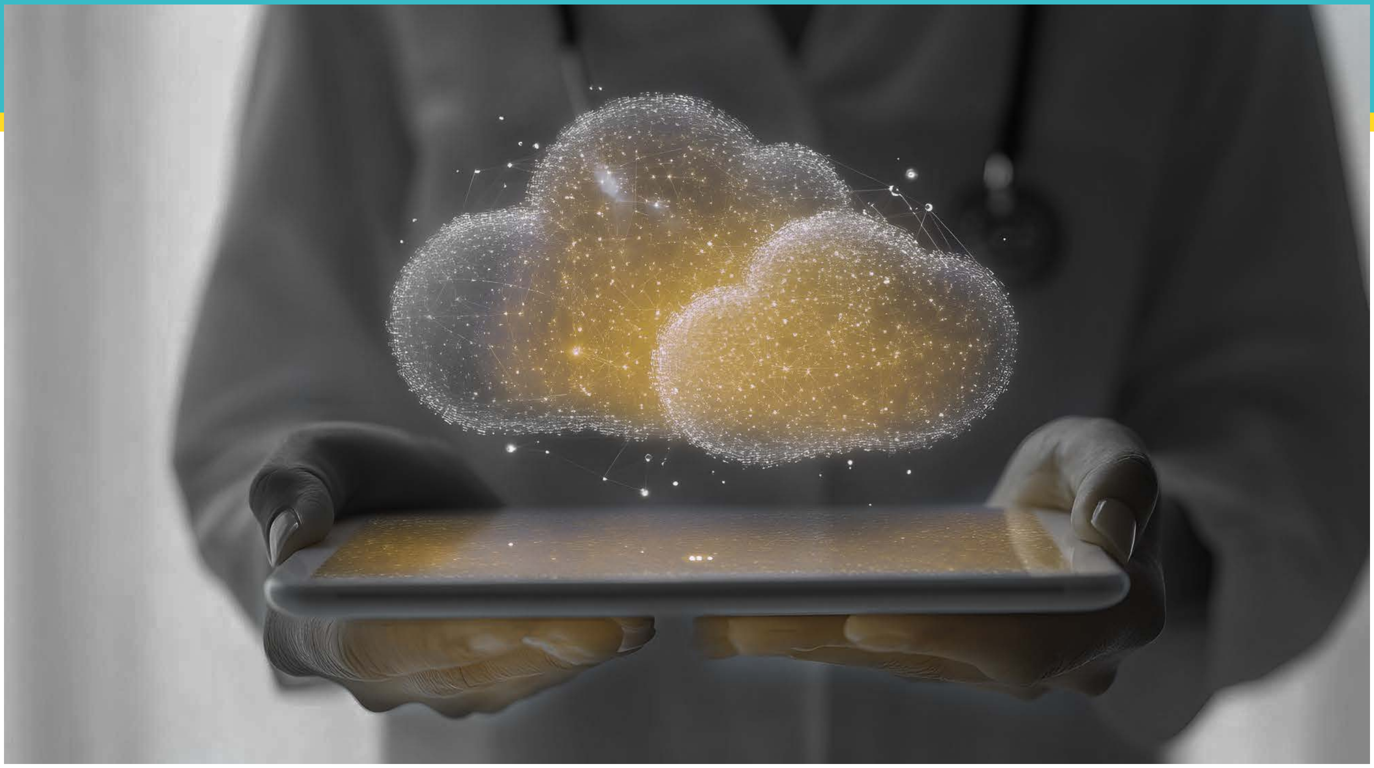
- ✓ Define business objectives and identify key workloads for the cloud
- ✓ Manage cloud spend: Utilize cost management tools (e.g., AWS Cost Explorer, Azure Cost Management)
- ✓ Implement multi-cloud and hybrid strategies to avoid vendor lock-in and optimize resource allocation
- ✓ Prioritize workloads based on criticality to balance performance and cost
- ✓ Use automation tools (IaC, AI, RPA) to standardize deployments and enhance efficiency
- ✓ Establish a governance and compliance framework for data access, policies, and audits
- ✓ Right-size cloud resources for performance and cost efficiency
- ✓ Implement multi-cloud strategies for flexibility and redundancy
- ✓ Use pricing calculators from CSPs to estimate and control expenses
- ✓ Adopt cost management software to monitor real-time spending
- ✓ Set up automated alerts for budget overruns
- ✓ Leverage AI and RPA to reduce manual interventions and streamline workflows

Day 61-90: Strengthen Compliance, Security & Foster Continuous Improvement

- ✓ Monitor storage tiers and shift data to cost-effective solutions
- ✓ Use predictive scaling to optimize resource allocation dynamically
- ✓ Conduct regular reviews to adjust and refine resource usage
- ✓ Adopt multi-cloud strategies to reduce reliance on a single provider
- ✓ Develop robust disaster recovery plans with frequent testing
- ✓ Integrate compliance and security into cloud operations
- ✓ Utilize Cloud Security Posture Management (CSPM) and Managed Detection & Response (MDR).
- ✓ Conduct thorough vendor assessments for regulatory compliance (HIPAA, HITRUST)
- ✓ Implement strong access controls and encryption for data security
- ✓ Audit third-party integrations and enforce least-privilege access policies
- ✓ Use automated security policies and AI-driven threat intelligence for continuous risk assessment
- ✓ Establish Key Performance Indicators (KPIs) for cloud success
- ✓ Stay informed on emerging technologies and best practices
- ✓ Encourage cross-departmental collaboration (IT, finance, compliance)

Looking to strengthen your cloud security and compliance strategy? Get a tailored roadmap designed for your organization's needs. *SCHEDULE A CONSULTATION* with our cloud experts today to take the next step toward a more secure and efficient cloud environment.

ClearDATA: Your Partner for End-to-End Cloud and Cyber Resilience.



ClearDATA stands out as the trusted partner for healthcare organizations navigating the complexities of cloud management.

With unmatched expertise in healthcare-specific compliance and security, ClearDATA ensures that your organization meets strict regulatory standards, including HIPAA and GDPR, while safeguarding sensitive patient data. Our tailored solutions span across AWS, Azure, and GCP, offering the flexibility to meet your unique organizational requirements and seamlessly adapt to your infrastructure needs at any stage of cloud maturity.

Through comprehensive managed services and continuous compliance monitoring, ClearDATA enables healthcare providers to focus on their core mission—offering exceptional patient care—without being burdened by IT complexities. Our proven track record in driving results speaks for itself. Organizations partnering with ClearDATA have consistently experienced improved operational efficiency with healthcare IT teams less than 20% of their time addressing cloud operations, up to 50% reduction in cloud operating costs, and enhanced compliance posture with an average compliance score of 93%, enabling them to stay competitive and innovative in a quickly evolving industry.

Experience the **ClearDATA Difference**

Enabled by the first and only software of its kind for healthcare, companies of all sizes gain full visibility, protection, and enforcement of security and compliance measures to secure PHI and other sensitive healthcare data in the cloud.

THE RIGHT EXPERTISE

ClearDATA's software and services were designed from the ground-up with healthcare providers and partners in mind. Rest easy knowing the healthcare industry's rigorous compliance needs are covered.

THE RIGHT SOLUTIONS

Whether you choose software-only or one of our managed services packages, ClearDATA's solutions can be tailored to your team's needs and work with the three major public cloud providers (AWS, Azure, and GCP) — which is exactly why healthcare organizations love them.

THE CLEAR CHOICE

Continuous compliance. PHI protection. Healthcare-focused CSPM. Wherever you are on your healthcare cloud journey, **ClearDATA is the clear choice for success.**

95 CSAT Score

"Excellent!" ★★★★★

HITRUST CSF Certified · HIPAA COMPLIANT · GDPR COMPLIANT

GxP Pharma Solutions · ITIL® · AICPA SOC

HIMSS North America PLATINUM Corporate Member · NIST · CIS SecureSuite® Membership

aws

delegate · JOHNS HOPKINS MEDICINE

Teladoc® HEALTH · Genentech A Member of the Roche Group

Omnicell® · ADVANTAGE Healthcare Services

children'shealth · EK Health Experience Better Managed Care™

...and so many more

Secure your organization's future with a robust and reliable cloud strategy. Discover how ClearDATA's solutions can empower your healthcare organization to thrive in the digital age.

ClearDATA.com   info@cleardata.com

CONTACT A CLOUD EXPERT

CLEARDATA®

MKT-0214 ©2025 ClearDATA