Healthcare Payers' Ultimate Guide to Transforming in the Cloud

A ClearDATA Resource

CLEARDATA™

Cloud catalyst. Healthcare protector.

Healthcare Payers’ Ultimate Guide to Transforming in the Cloud

Every year it seems the American healthcare system becomes increasingly competitive, with heightened regulatory scrutiny. Payers are not immune to these market pressures. As we see more health insurance providers evolve from using legacy, on-prem solutions to advanced cloud strategies and infrastructures, it’s critical to prioritize the smoothest digital transformation as possible.

The modern public cloud has the power to solve many technology requirements, but it still requires expertise to properly architect a well-designed solution. With the right preparation and consultation, you will be well positioned to fully leverage modern technology and unlock your organization’s full potential.

Inside:

1. **Unsticking Your Cloud Journey** **1**

2. **How to Pursue Digital Innovation and Reduce Risk** **3**

3. **How to Use Emerging Technologies in a Secure Healthcare Environment** **6**

4. **How Payers are Leveraging AI and Machine Learning to Improve Member Engagement** **8**

5. **Common Mistakes Payers Make in Their Digital Transformation Efforts** **10**

6. **Payer Case Studies: Improve Member Experiences While De-Risking the Cloud** **12**

Unsticking Your Cloud Journey

While most companies now understand how cloud computing will transform their business, some are finding themselves stuck on their public cloud journey — feeling cautious about making the switch or expanding further into the public cloud. What fosters this underlying apprehension, and what can a healthcare organization do to unstick its cloud progression?

Healthcare organizations can use the public cloud to accelerate speed to market for new applications, leverage machine learning for improved data analysis, improve on security, compliance, and privacy rigor, and ultimately improve customer, patient, and member experience. While action makes more fortune than caution, a traditional IT procurement cycle mindset persists that sometimes inhibits the adoption of the cloud. Capacity planning and ongoing maintenance, both at the software and hardware layer, can be difficult with on-prem data centers, and even worse, mistakes are expensive. It is these limitations, and the classic on-prem mentality they conjure, that conflicts with the cloud and its capability to offer a limitless amount of IT resources and a more economical pay-for-use model.

Sticking Point #1: Expectations Around Migration

But even with all the benefits public cloud-based applications and services have to offer, knowing how your business can best reap them is not always straightforward. The big cloud journey glue trap is often the false expectation that whirls around the lift-and-shift strategy. It can be an unproductive undertaking that launches an organization's existing bloat into the cloud: logs, malware, traditional server database architecture, and the like. And then you'll hear the classic lift-and-shifters' complaint: "Hey, I moved hundreds of my assets to the public cloud, and now it's more expensive!"

Replicating antiquated on-prem processes won't deliver the value that you're looking for when adopting cloud technology. Business leaders must think about how the cloud is different and how that will benefit their organization and help them meet and exceed their business goals and objectives. Running a tabletop exercise to map your current processes to the way the public cloud works is essential. This requires getting interdepartmental stakeholders in a room to talk about security incidents or change management. If you do this upfront, you will get ahead of application and services gaps that may exist during any cloud transformation activities. Maybe you'd like to migrate the new version of the application. Walk through it: how it works inside your data center today—and then how it will work inside the cloud. If your exercise reveals the process is the same on-prem as it will be in the cloud, you've done something wrong. The reason why: that tabletop exercise should be able to identify what processes should or could be changed or automated. And hopefully, most of the processes can be automated. For the ones that can't be, consider alternative services that may drive down cost and complexity, or investigate cloud roadmaps for when those processes may be automated down the line.

Sticking Point #2: Business Associate Agreement Negotiations

A second area where organizations get stuck is in finalizing the required Business Associate Agreement (BAA) all covered entities and their business partners who engage with PHI are required to have. Can you negotiate your agreement? Do you have the right shared responsibility model? Do you have an agreement in place with every third-party vendor that stores, processes, or transmits PHI? It's important to find a partner who understands the BAA and can negotiate it to specifically contain that amount of shared responsibility your organization needs.

Sticking Point #3: Reputation Concerns

A Chief Information Security Officer's (CISO) concerns about the cloud — and his or her reputation — may also be a factor for the cloud journey getting stuck. Migrations require the confidence and cooperation of the CISO and compliance team who may have built their careers around creating very secure environments inside of facilities — whether it's data centers, co-location facilities, or even

SaaS applications. Many CISOs are not certified in public cloud technologies, and HITRUST certification is new to a lot of these organizations. In fact, HITRUST, along with other standards, are rapidly evolving, only recently incorporating public clouds like Google Cloud within its scope. One of the key considerations when working with a CISO on public cloud adoption is how to keep up with changes in healthcare regulations and policies, and how to map those back to the cloud services adopted. It can be a wise move to dive into the expansive security advantages available in the cloud with a managed services partner to get to the answers you need to proceed with confidence rather than wander in alone.

Unsticking Your Cloud Journey

The pressure to scale and innovate can also make things sticky, but a partnership with a cloud service provider can show you — component by component — where you can optimize and accelerate your operations. This process enables the build out of healthcare compliant reference architectures that allow for auto scaling. For example, in the payer market, during open enrollment season, traffic surges and systems become incredibly overloaded. But by being able to build out a reference architecture that allows the payer's system to auto scale, enrollment services and other consumer-facing functions just continue to deploy automatically. There are no worries about handling traffic spikes, and you can provide cost predictability during those peak periods.

Maybe your sticking point is you are sold on the cloud, but you're not sure how to sell it to your fellow executives. First you can emphasize that by leveraging the efficiencies of the cloud, your organization will gain a newfound ability to focus itself on its core mission. Then, preach how the cloud can help you:

- Streamline operations by reducing the responsibilities related to maintaining capital infrastructure.
- Keep current with regulatory changes and be able to map cloud technology back to those regulations.
- Stay on top of all new innovations, no matter how fast they come.

Example: Well over a thousand major changes inside of one public cloud last year alone that had a direct effect on security, privacy, and compliance of sensitive data, such as PHI.

If you work at a provider, for example, you can put the cloud migration argument this way: "If I'm not spending half of my time maintaining underlying infrastructure, I can focus on changing our CapEx model to an OpEx one, over time. I can shave my overall healthcare IT spend from 3.7% to 3.2% — which is a massive cost reduction! And I can do it all over time by automating lots of our processes, not just putting workflows in cloud."

How to Pursue Digital Innovation and Reduce Risk

While healthcare has begun investing more heavily in digital transformation during recent years, not everyone has fully committed to the path of innovation. The biggest change most healthcare organizations have experienced over the last few years has been the transition to electronic health records — a time-consuming and costly initiative that has taken resources away from innovation initiatives. Meanwhile, industries like retail and banking continue to push the envelope and have reached a level of digital maturity that has transformed the way they do business.

But the tide is turning. Disrupters like Google, Apple, and Amazon are investing heavily in the healthcare industry, opening up new possibilities and, even more so, posing a real threat to healthcare organizations that remain stagnant and risk-averse.

IT leaders know digital transformation is necessary and that nobody in the healthcare industry can afford to put digital innovation on the backburner. Instead, they need to approach it strategically and with a solid technology roadmap in place.

This guide will discuss some of the digital innovation initiatives that are transforming healthcare, the new business risks these initiatives can introduce, and a few key strategies healthcare organizations can adopt to stay competitive and reduce risk.

Transformative Technologies

One of the biggest misconceptions about digital innovation is that it involves taking an analog process and simply making it digital. This is not the case. True digital innovation is transformative, which means one of two things should happen: it completely changes the way a business functions, or it revolutionizes the user experience. In some cases, both happen.

While some healthcare organizations have seen huge success in their transformation initiatives, this type of innovation has been hard to come by broadly in the healthcare industry, mainly for two reasons:

- **Lack of resources.** Over the last several years, many healthcare IT teams have been busy keeping their on-prem infrastructures up-to-date, compliant, and safe from vulnerabilities, leaving little time or money for innovation initiatives.
- **Risk aversion.** Privacy, security, and compliance continue to be critical concerns among healthcare organizations — and with good reason. The number of data breaches happening within the healthcare sector are reaching record highs, and electronic health records are three times more valuable than records in other industries. Meanwhile, privacy regulations are getting more stringent. These facts, combined with a lack of time and resources, have made it hard for IT leaders to venture into digital innovation without fear of putting security and compliance at risk.

Leaders both within and outside the healthcare sector are responding by adopting next-generation technologies like cloud computing, machine learning, and virtual reality to create healthcare solutions that improve efficiency, communication, and patient outcomes. Here are a few examples of the digital innovation initiatives happening within healthcare:

- **Wearable devices and remove monitoring.** Now more than ever in the wake of COVID-19, the ability to continuously monitor a patient's health has become increasingly critical. The Apple Watch Series 6, for example, now offers two FDA-approved heart features — an abnormal heart rhythm alert and an electrocardiogram (EKG or ECG). Other wearable devices such as sweat meters and oximeters are being used to treat conditions like diabetes and respiratory illness. Juniper Research forecasts that 5 million individuals will be remotely monitored by healthcare providers by 2023.
- **Digital assistance.** The rapid adoption of digital personal assistants like Alexa, Siri, and Google Home has opened a slew of possibilities for patients and healthcare organizations. Mayo Clinic has introduced a free Mayo First Aid skill that

provides voice- driven, self-care first aid instructions to patients through Alexa, Google Home, and voice-power web chat platforms. Nimblr, an artificial intelligence (AI) startup, has developed an AI assistant named Holly that helps both providers and patients with medical appointments. The company's platform can even integrate with Alexa, which allows patients to book and reschedule appointments using voice commands.

- **Virtual Therapeutics.** Augmented reality (AR) and virtual reality (VR) technologies are being implemented and scaled across healthcare applications, as with behavioral health company BehaVR. These technologies are not only being used in care management to treat conditions such as pain management, PTSD, and bipolar depression, they are also being used for training and education purposes. This includes VR-based operating room simulations that train surgeons, and AR-based apps that assist elderly patients with medication management.

Five Risks to Avoid

Although each of these digital initiatives is changing healthcare as we know it, they also open healthcare organizations — and their customers — to a whole new set of business risks, most of which involve security and compliance. However, when managed correctly, digital innovation initiatives can be safe and successful. IT leaders simply need to be proactive and prepared.

The following are five risks today's healthcare organizations need to avoid when working toward digital innovation:

1. **Not Knowing What You Have**
   Before a healthcare organization considers taking on any digital innovation initiative, it needs to have a thorough understanding of its end-to-end system. This includes all networks, devices, data assets, and data flows. IT teams are continually adding to and reconfiguring their networks, so it's easy to lose sight of the most recent device addition or how a configuration change affects the flow and access of sensitive data. The IT staff need to maintain a detailed record of everything connected to their networks and systems — across locations, hosting models, and user populations (i.e., staff, contractors, patients, etc.). This also includes unrelated systems, such as heating, ventilation, air conditioning (HVAC) and point of sale systems. Conducting a real-time data flow analysis and assessment of all network assets is the first step toward mitigating security risk. If you aren't sure how, there are third-party consultants exclusive to healthcare that can assist you.

2. **Security Gaps**
   When it comes to security and compliance, too many healthcare organizations focus on point-based security controls instead of pervasive security. While IT teams may address security and compliance in individual technologies such as an MRI machine or a claims system, most don't take the time to see what needs to be done holistically. This can leave an infrastructure open to security gaps and unexpected vulnerabilities. Because security standards are constantly changing — sometimes on a daily basis — IT leaders need to ensure their entire infrastructure is resilient by adopting a holistic compliance strategy that closes any potential gaps.

3. **Data Sprawl**
   With digital liquidity increasing from more people using more devices and applications, it is difficult for healthcare organizations to have a handle on where their data is, which means it is difficult to keep it protected. This is especially true as organizations pursue data-rich initiatives like continuous monitoring. Handling the amount of data coming in and knowing what to do with it is a huge challenge for today's healthcare organizations. IT leaders need processes in place to identify what data they have, where it lives, and how it is classified from a privacy and security standpoint.

4. **Role Drift**
   As any healthcare IT leader knows, recruiting top talent can be challenging. However, digital innovation requires digital skills. When taking on a new initiative, having a qualified staff and access to knowledgeable partners is critical for maintaining data security and compliance throughout the initiative. It is important that organizations implement policies and procedures that closely monitor IT roles and who has system access. Oftentimes, IT leaders forget to remove access after periodic changes in duties or offboarding. Reviewing roles and access privileges in quarterly formal meetings can help mitigate this risk.

5. **Lack of Agility**
   Digital technology continues to advance at an increasingly rapid pace, and healthcare organizations need to be sure they are prepared to keep up with the rate of change while still meeting regulatory requirements. This means having the proper resources, equipment, and expertise. Agility can be

difficult for IT teams that are tied to antiquated legacy systems, capital expenses, and daily maintenance tasks such as hardware ordering, inventory levels, and capacity. Ordering a new internet cable or server, for example, can delay a project for several months. Because of this, many healthcare organizations are moving at least part, if not all, of their IT infrastructure to the cloud. This not only enables agility, but it also allows for scalability, faster time to market, and frees up more resources for core competencies and innovation initiatives.

Strategic Solutions

Although there are several strategies IT leaders can adopt to avoid these common risks, there are two best practices every healthcare organization should consider:

- **Adopt a Zero Trust Framework**
  Maintaining security and compliance in today's digital landscape isn't easy, but it is possible. Although healthcare organizations have historically relied on network and user permissions to manage access to secure data. Instead, Forrester's Zero Trust Security Playbook offers detailed guidance on how to implement a Zero-Trust strategy. This requires IT teams to implement a series of Zero Trust security measures that include people, workloads, devices, networks, and data.
- **Team Up With Partners**
  Many organizations are finding that the only way to free up IT resources for digital innovation and ensure their infrastructure is secure is by augmenting their team. Service providers that have deep expertise in data security, healthcare compliance, and cloud computing can help alleviate a lot of the daily maintenance, security, and compliance responsibilities that typically burden IT teams. Leveraging the expertise of trusted partners is a strategic move any non-tech company should consider when taking on any digital innovation initiative.

The Time Is Now

As healthcare organizations look at what's happening in the market, it is hard to ignore the call for digital innovation. Consumers are asking for it, and the industry is already feeling the pressure from COVID-19, external forces, and industry disruptors. To remain competitive, today's healthcare organizations need to ask themselves: Are they willing to develop the type of digital experience their patients want, and are they equipped with the technologies and expertise necessary to enable them?

While digital innovation often introduces a whole new set of business risks, the reality is that the biggest threat to healthcare organizations is not responding to the changes happening around them. Companies like Blockbuster and Sears learned the hard way what can happen when you fail to innovate your business model.

Instead of being afraid of digital innovation, healthcare organizations need to be informed, prepared, and strategic. Digital transformation is coming, and healthcare IT leaders have a prime opportunity to help their organizations be a part of it. With the right resources, partners, and strategies in place, IT leaders can refocus their efforts on innovation and play a key role in the long- term success of their organizations.

How to Use Emerging Technologies in a Secure Healthcare Environment

As you fly over the translucent concrete skyscrapers of a domed city in a carbon nanotube plane flown by a pilot wearing a trans-cranial, neural sensing headset, you may begin to contemplate the wonders of emerging technologies—and the competitive advantages they can provide.

As an empowering force behind emerging technologies, the public cloud has gone from what was once just a technical capability to emerge as a strategic priority. Today, numerous players across the healthcare spectrum are pushing past the computing equivalent of the sound barrier to create stronger, faster tech in the cloud. Here's what technologies are flying high right now and how they can benefit healthcare organizations like yours.

Tearing the Lid Off Container Technology in Healthcare

Designed to let software-on-the-move operate from one environment to the next, container technology is the whole runtime environment in a single package. Many see it as the next evolution of cloud management as we move from physical servers to more virtualized ones. In fact, according to Gartner, 85% of enterprise workloads will run on containers by 2025, whereas less than 30% were in 2020.

But why the sudden acceleration in adoption? First, there's the budgetary benefit. Many organizations are using containers to better employ existing resources and to drive much greater horizontal scaling. For example, insurance providers see much larger traffic and data around open enrollment periods. While cloud economics can burst out to accommodate the higher traffic, containers allow it to burst out even more efficiently. There's also a development benefit. As developers create new features and services, containers allow them to do it in one place.

Kubernetes: The Maestro of Container Technology

Building on the success of containers is Kubernetes, an open-source platform that gives system administrators much more control over their container environment and automates many processes. Not only does Kubernetes offer more standardization for managing containers, but it has also become the forefront of orchestration—making it much easier to get started. Organizations embracing Kubernetes environments find that it's much simpler to add entirely new applications and scale new services—resulting in improved time to market.

In addition, by strengthening and standardizing security controls, Kubernetes enforces security policies across all applications. Not only does that remove policy conflicts, but it also eliminates a lot of the compliance and security requirement concerns from the development teams, letting them focus on their work in a more risk-free environment.

Making Natural Language Processing Second Nature

Software developers are locked in a primordial challenge. The process of bringing order to chaos began at the dawn of creation and has never ceased. Natural language processing (NLP) is the continuing echo of that effort—extracting relevant medical information from the data disarray. Some good examples:

- **Optimizing the patient matching process for clinical trials.** By speeding through identifiers in previously difficult-to-decipher information (patient forms, doctor's notes, test results, etc.), NLP can create larger data sets to make it easier to find the right trial candidates. Previously, the alternative would be manually rummaging through tens of thousands of medical records.
- **Improving the call center experience.** Insurance providers take thousands of calls daily. From the caller's perspective, it may not always be an optimal experience. NLP can help by processing the call live, evaluating customer sentiment, and determining if the operator needs to improve the call tree setup. If customer frustration is detected, the conversation can be flagged for a different approach or a more suitable handler.

Distributed Tracing: Putting an Eye on PHI

It's impossible to secure data if you don't know where it is. But how do you avoid the third rail of security and compliance if your healthcare organization does not have a 100% accurate and up-to-date PHI inventory? Distributed tracing tools can help. They can provide additional visibility by detecting, tracking, and locating PHI within the microservice architecture—helping to close that gap. With a more accurate inventory, you'll know which services are processing PHI, and you can take additional steps to secure them. That better inventory awareness mitigates a potential security incident by going back and verifying exactly which patients were potentially impacted by it. By narrowing the scope, you don't have to—for example—reach out to a million patients whose records were breached, but only the 500 patients who were potentially impacted. That's a much less expensive issue.

Every once in a while, a technology is hatched out of the creative ether that takes the world by storm. Kubernetes is reshaping the future of app development and management, creating a thriving ecosystem. The evolving faculty that machines have to interpret our speech and documented thoughts, opens new possibilities for the interactions between computers and people. When it comes to these emerging technologies, education is the key to approaching the future fearlessly. An experienced, healthcare-exclusive cloud services provider can supply a jumping-off point into studying this neo-tech and exactly how it can be applied to different healthcare verticals. That partnership will lead you into a discovery process that builds expertise in your team and creates a more independent ability to innovate in the cloud while remaining secure and complaint. Life is all about what's next and fostering a culture of inquiry will help your organization embrace all that the cloud has to offer and broaden the scope of what technology can do to improve the lives of patients.

How Payers Are Leveraging AI and Machine Learning to Improve Member Engagement

Across the country, a growing number of payer organizations are transforming the way they engage with both their members and the providers their members seek services from. To do so, payers are investing more in innovation, with one of the core focus areas being artificial intelligence and machine learning. Ultimately, their goal is to take advantage of the digital transformation these and other technologies are enabling to improve and personalize member experience dramatically while creating greater value and driving operational efficiencies. The pandemic accelerated the digital transformation in healthcare and is it estimated that healthcare averaged two years' worth of digital transformation in just the first two months of the pandemic.

In this article, we will look at some of the specific ways in which payers are using machine learning (ML) and artificial intelligence (AI) to do that and more.

Improving Outcomes for Everyone

At a time when consumers (patients) have come to expect the kinds of easy, always-on, and personalized experiences they're used to getting in every other aspect of their lives, patient experience is critical. We all know that the traditional healthcare experience is not the same experience that you may get in other personalized industries in your life today. To deliver better experiences, payers have recognized the need to focus on two key areas.

The first is ease of use, which includes things like ensuring customers always understand what's in network and what's not, or what the status of a claim is. The second is ensuring their services are available on demand so that customers have around-the-clock access to the systems, people, and processes they need. Underlying both of these expectations is a need for data-driven insights and digital innovation that create value.

When payers take advantage of machine learning and artificial intelligence, they're not only able to meet the patient's growing needs and expectations, but also deliver better outcomes for providers and patients alike. That's critical and just one of the reasons why 54% of healthcare professionals expect the widespread adoption of AI across the industry by 2023.

To understand how payers are using machine learning and artificial intelligence to increase engagement and drive better outcomes, let's take a look at some real-life examples of how this technology is being put to use.

Reducing Hospital Readmission Rates

Some payers are using machine learning to look at claims data across multiple electronic medical records to try to help providers reduce hospital readmissions. Reducing the rate of infection following surgery is a good real-life example. Savvy payers are using machine learning to analyze vast claims data sets to see when issues like inflammation and blood clotting occurring after a surgery. They can then see which medications were used to treat those issues and if they were effective. Ultimately, they can use this data to predict whether or not a patient is likely to have to get re-admitted to the hospital following surgery.

By delivering those insights to providers, they're not only demonstrating greater value, but also empowering providers to take the steps necessary to try to prevent any hospital readmissions that can be avoided. In doing so, the patient, the provider, and the payer all benefit.

Revenue Cycle Management

Some payers are using machine learning to figure out how soon a hospital will get paid for services rendered based on a particular diagnosis. In other words, they're determining how quickly patients will receive a letter in the mail that says what their financial responsibility is and how quickly they'll actually pay it. Payers are also using machine learning to help providers understand their patients better, including which ones are most likely to be no shows and which are likely to receive services and not pay for them.

Improving Clinical Efficiency

Healthcare payers are also focusing on improving clinical efficiency and outcomes. Here they're using machine learning to look at which treatments deliver the most clinically effective outcome at the lowest cost.

Fraud Detection

Fraud detection is another use case for payers. Medical identity theft was at an all time high in 2020 with double the number of cases in 2019. It's important for payers to know if the person submitting a claim is in fact who she says she is and actually received the surgery or treatment she's claiming to have. With real-time authorizations that work in a way similar to the banking industry model, payers can ensure the authenticity of a claim.

Machine Learning Gets Results

Although healthcare organizations haven't typically been among the early adopters of new technologies, this risk-averse group is finding security in the public cloud, often by partnering with third parties. Doing so is allowing payers to explore the potential that machine learning and artificial intelligence bring to improve outcomes across their member base and within their own financial centers. In fact, these days, payers are among the growing number of healthcare organizations using machine learning and artificial intelligence to change almost every aspect of the healthcare industry. Importantly, they're doing so to not only engage providers and patients and deliver a better overall experience and better outcomes, but also to drive efficiencies and lower their costs.

While some of the ways in which payers are already leveraging machine learning and artificial intelligence include reducing hospital admissions, managing revenue cycles, and improving clinical efficiency, that's just the tip of the iceberg in terms of what's possible. In the not-too-distant future, we expect to see major changes as healthcare increasingly happens through mobile interfaces and machine learning enables data-driven diagnoses.

For payers more specifically, the ongoing adoption of machine learning and artificial intelligence will mean that it becomes much easier for patients to achieve better health outcomes as well as understand things like if their treatments are in network or not, or how much they'll need to pay out of pocket. In the process, it will also dramatically reduce the amount of time it takes for claims to be processed.

Ultimately, these and other benefits of artificial intelligence and machine learning are a win for payers, providers, and patients alike.

Common Mistakes Payers Make in Their Digital Transformation Efforts

Introduction

Healthcare payers face a variety of pitfalls when implementing digital transformation efforts. These common mistakes can have a big impact on operational efficiency and business risk. Know these common mistakes and avoid them to ensure success in digital transformation.

Common Mistakes Observed in the Payer Market

Digital transformation tools can help you store data in the cloud securely, comply with federal and state healthcare regulations, and increase transparency in healthcare quality and costs. However, when improperly implemented, digital tools can hinder rather than help you. In fact, 93% of organizations are concerned that human error will cause a data breach.

Some of the common mistakes seen among healthcare payers approaching digital transformation include:

- Focusing on their app or solution first, and then trying to build security and compliance around them as an afterthought in the process.
- Not including key stakeholders throughout.
- Not engaging their vendor management organization early enough.
- Security risks posed by insider access. 32% of organizations have unnecessarily privileged access for users that don't need it.
- Trying to succeed in digital transformation alone instead of tapping the expertise of partners.

Digital transformation tools have the power to reshape how you serve your customers, while also helping you improve operational efficiency. But payers should work to avoid these four common mistakes listed below, as they will slow down progress in transforming your organizations and open you to costly compliance issues in the long run.

Including Security and Compliance Only as an Afterthought

As with almost anything in healthcare, you must remember to include compliance and security in every digital transformation effort. Too many organizations concentrate on building their app or solution first, and then try to fit compliance and security to the solution. Compliance and security need to be steeped into the culture of an organization and the products and services you use, as well as front of mind when you're architecting your digital environment. You should partner with third-parties who have compliance and security baked into everything they do.

Not Engaging Stakeholders

You must engage all stakeholders throughout the digital transformation process. If not, your digital transformation efforts are likely to have blind spots and siloed information that erode your ability to succeed. The sooner you engage key stakeholders, the more successful you will be. That's especially true for executive staff such as the CISO (Chief Information Security Officer), who is legally obligated to be sure any security risks are taken into account in your planning and implementation.

Involve Your Vendor Management Organization

One of the items that ends up being the biggest hurdle with payers is the contracting process. Payers, particularly large insurance companies, usually have a large vendor management organization (VMO) in play for contracts, business associate agreements, and other legal documents. You want to involve that group early on, so its team can advise ways to speed time to contracting and thus, time to value. Ask your VMO what it needs for legal, procurement, IT or other and business units early to ensure success.

Not Leveraging the Expertise of Others

Other industries have mature digital transformation technology, so work with partners who have already achieved success to help you. You don't have to "reinvent the wheel." Tapping others who already have digital transformation expertise will not only save you time and money but also help ensure your efforts are successful. Forbes labels these people as "digital achievers," and they may not always be found only in an IT department. Whether they come from within or outside of your organization, these digital transformation "achievers" have the unique ability to understand the basics of working and competing in a world revolutionized by technology and can solve problems from the customer's perspective, not just their own.

Digital Transformation Challenges Payers Face

As they grow, many payers struggle with how and what data to migrate to other systems. They grapple with what should be in their data center and what should move to the cloud. Some believe they can do the job themselves, while others realize they need to turn to look for outside assistance.

Digital Transformation Can Pay Off

Without digital transformation, both payers and providers face a bit of a bleak future as healthcare costs, especially for chronic care, continue to rise. The Centers for Disease Control states that 90% of healthcare costs are spent on chronic disease and mental health conditions. Personalized care through digital transformation can help prevent or better manage chronic disease. The end result is healthier, happier members at a lower cost.

The impact of the failure to pursue digital transformation efforts, such as personalized care, can be illustrated by the statistic shared recently by CNBC that indicates two-thirds of people who file for bankruptcy cite medical issues as a key contributor to their financial downfall. Many Americans who have health insurance can't even afford to pay the out-of-pocket expenses that accompany their insurance plans. Because care is costly, many people wait to seek care until later in an illness where more expensive hospitalizations are required versus the more engaged preventative care possible with digital technologies.

But when done correctly, digital transformation can provide you with big benefits. It can increase transparency, improve healthcare quality, reduce costs, and provide new ways for you to connect with consumers.

Digital transformation programs can increase your profitability. Research shows the high revenue, high margin business that many in the healthcare industry traditionally have relied on is going away, but the digitally transformed organization that is operationalizing data to the cloud provides greater efficiencies. Either way, digital transformation can give you a competitive edge over others in your market.

The New Digital World

Digital transformation is changing the way payers do business and revolutionizing patient care in an era where the economics of healthcare are shifting. As patient outcomes and healthcare costs come under increasing scrutiny, payers must be able to manage their operations in as efficient and transparent a way as possible while still meeting the many security and compliance regulations governing them.

Improve Member Experiences While De-Risking the Public Cloud

Transformation of the Member Portal to Improve Member Access to Data

Client A statewide, New England-based health insurance provider serving 3.2 million members

This organization sought to reimagine the interactions users experienced through their member portal. They aimed to give those members direct access to their information to improve engagement. However, building a more interactive member portal would require migrating from their data center and deploying infrastructure in the cloud while keeping PHI protected at all times. By engaging ClearDATA to provide a DevOps automated healthcare platform of software and services, they were able to design a solution that safeguards PHI as it flows through the member portal system. As a result, the company has gained richer, actionable data-driven insights that allow them to engage more effectively with their members.

Their Vice President and Chief Technology Officer summarized the value they harnessed via their ClearDATA engagement:

"Although cloud is strategic for us, the ability to be experts on the cloud and cloud compliance is not necessarily strategic for us. Our business is healthcare, and we want to ensure that all of our energy is focused on what the right things are for our members, and how we can best address their needs in the marketplace."

The Transition from Transactional Model to Personalized Care for Member Wellness

Client A statewide, consumer-focused, nonprofit health plan

This health plan committed to transform their organization from transactional health insurance to one focused on personalized wellness for their 2.8 million members. They aimed to do this by embracing cloud to gain insights and capabilities through robust enterprise analytics. However, siloed data across over a dozen business divisions made collaborating to glean insights difficult. As a HITRUST-certified organization, ClearDATA offered a secure platform for the organization to innovate at scale and harness the power of emerging technologies – such as advanced analytics - in the public cloud. ClearDATA also offered them a multi-cloud negotiated Business Associates Agreement (BAA) to address a variety of needs and liabilities across their complex organization. By implementing a secure and compliant cloud via ClearDATA, this health plan was able to turn its focus toward strengthening cross-divisional collaboration to achieve unparalleled consumer experience.

The plan's Chief Architect reflected:

"With ClearDATA, those obstacles of thinking about compliance are gone for me and my team. Being able to wrap our analytics platform with the protection of the ClearDATA platform allows us to access capabilities within the cloud that we would never have access to on our own."

Capitalize on a Secure, Compliant Cloud to Improve Member Engagement

As your strategic partner, ClearDATA will help you harness the power of the cloud so you can focus on your business objectives while maintaining your security and compliance posture. ClearDATA can help you embrace digital transformation and move from completely on-premises to cloud, or hybrid cloud infrastructures, for improved agility, business insights, and cost optimization.

Accelerate Your Cloud Journey

We meet you where you are on your cloud journey. Our proven healthcare expertise paired with our team of certified cloud experts can help you plan your cloud journey and scale for the future.

Secure and Protect PHI

Healthcare's complex compliance frameworks require constant time and attention—time that is taken away from your team to address your business objectives and goals. Let us take that burden from you with our deep experience mapping standards and regulations such as HIPAA and GDPR and configuring the latest cloud technologies in a compliant manner to keep sensitive data secure and protected in the cloud.

De-Risk the Cloud and Drive Innovation

Cloud-based digital engagement and analytics applications offer the flexibility, scalability, and affordability that healthcare organizations need for the populations they serve. Our healthcare and cloud expertise combine to bring you software and services that ensure your teams can focus on your core competencies and leverage the latest cloud technologies like machine learning and advanced analytics, while we take care of security, privacy and compliance in the cloud.

ClearDATA.com | (833) 99-CLEAR

Partner with the Healthcare Cloud Experts

The team of ClearDATA experts can be a force multiplier for your organization to take advantage of emerging technologies in a safe, secure, and compliant manner. Our partnership with large health insurance plans and providers has helped them leverage the latest cloud technologies in a secure and compliant manner. Let's talk about what ClearDATA can do for you.

Speak with an Expert