ANALYST BRIEF
Sponsored by: Pure Storage

A strategically planned cloud journey accelerates applications, encourages data flexibility, and enables innovation across the enterprise.

How Healthcare Payers Can Strategically Plan Their Cloud Journeys for Enterprise Growth

September 2023

Written by: Jeff Rivkin, Research Director, Payer IT Strategies

Introduction

Healthcare payers have been implementing cloud data storage solutions for the past decade. As cloud providers demonstrated their ability to provide enterprise-grade solutions to this market, many payers moved to a cloud-first/cloud-only approach.

To ensure operational excellence for their members, providers, and internal constituents, payers need to examine specific applications, workloads, security, and privacy standards as they evaluate cloud solutions. A cloud deployment should not be viewed as a destination but as a journey.

This journey takes costs into consideration, but more importantly, the journey is a conversion to an enterprise data ecosystem that comprehensively considers:

- Hosted datacenters
- On-premises storage
- Edge computing
- Cloud platforms
- Storage as a service
- Software as a service
- Containers and Kubernetes
- Cloud bursting

Traditional payer applications — such as enrollment, claims, billing, and revenue management — have grown to include clinically focused applications such as wellness and care coordination; hospital admission, discharge, and transfer tracking; and the creation of internal electronic health records. This expansion allows clinical data to join administrative data in the payer scope, and the data sets are merged into a comprehensive patient-centric record.

AT A GLANCE

WHAT'S IMPORTANT

Establish an overall vision for the data ecosystem, then modularly implement sections of the architecture.

KEY TAKEAWAY

The standardization of data formats, consumer dissatisfaction, payer-provider organizational shifts, and whole-person approaches to healthcare is moving the needle toward a more integrated, less automatic journey with cloud paradigms.

This approach continuously segments and categorizes members/patients to provide quality customer service in the days of the consumerization of healthcare and health insurance. Doing this allows customer service, enrollment, claims, and care coordination to access and use the same base of data to profile members and provide the level of service they require. To help payers achieve these goals effectively, cloud and datacenter strategies need to optimize a high-availability, low-latency solution.

Just as a 360-degree understanding of members evolves to become more comprehensive, so too should a payer's cloud journey.

Benefits

The standardization of data formats, payer-provider organizational shifts, and whole-person, value-based approaches to healthcare is moving the needle toward a more integrated, planned journey with cloud paradigms. Payers are trying to reduce risk by deploying flex storage capacity based on demand and by implementing data replication strategies as a general course of action.

An enterprise approach cannot be done overnight. Payers need to ask:

- What can we do today?
- What positions us for the future, where do we want to go, and what are we waiting for?

Establishing an overall vision of where the enterprise approach is going and then modularly implementing sections of the architecture seems to be the most appropriate course of action. Pulling back from the "cloud everywhere, cloud now" mindset seems prudent.

Gather the requirements into a structured strategy, and leverage outside needs to evaluate and deploy by using the considerations in the section that follows.

Considerations

To realize consistent multicloud automation in an enterprise operating model, organizations should answer the following questions:

- Does the overall solution and its phasing consider capabilities from both the provider and payer perspectives, given that payers are moving toward "payvider" models in search of solving the cost-of-care challenge?
- With interoperability as an ongoing priority, are the data exchange solutions under consideration intended to be implemented by the organization or will they require similar implementation by provider partners?
- Will providers and other data partners (e.g., social determinants of health [SDOH] sources) embrace the solution chosen by the organization, or will they wait for standards that allow them to implement one solution for all payers?
- Can the member-360, claims, enrollment, and care management systems integrate seamlessly?

- Can the organization handle the complex roles of prior authorization within equally complex, value-based, payment contracting?
- Is the organization establishing an environment that allows a spin-up of innovative applications? These include:
  - Artificial intelligence (AI) test beds for risk assessment, fraud/payment integrity, and population health
  - Merger/acquisition data and workflow consolidations
  - Taming high-volume data tsunamis from remote monitoring, care anywhere management, and genomics
  - Integrated prior authorization requirements inspired by the 2026 CMS mandates
  - Conversational and generative AI
  - Real-time adjudication of claims and authorizations
  - Expansion of member/patient engagement and experiences
- Have you considered the transparency requirements necessary for any AI-focused set within this operating architecture? In detail:
  - **Data privacy.** This concerns the correct treatment of data, such as whether personal information is shared with third parties. With the rise of big data, data privacy has sparked a heated discussion, since it is both necessary and risky. On one hand, data availability provides the foundation for improved AI system performance, but without enough training data, AI models are potentially biased and unable to generalize unseen data sets. On the other hand, careless release and handling of private data are extremely risky and can result in privacy breaches, trustworthiness, penalties, or civil suits. The United States Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act (ECPA), and the Children's Online Privacy Protection Act (COPPA) are just a few examples of data privacy regulations. For AI to work efficiently, its algorithms need to access a large amount of data and healthcare information about policyholders, some of which may be sensitive, thus raising data security concerns for insurers.
  - **Security.** Data protection refers to any procedure that uses suitable technological or organizational methods to safeguard digital information from unauthorized or illegal access, corruption, destruction, damage, or theft across its full life cycle. The European Union's General Data Protection Regulation (GDPR) is the world's strongest privacy and security regulation. It puts duties on all enterprises that target or collect data about people in the European Union. As stated previously, storing large amounts of data in a single place can make it easier for that information to be targeted by hackers and used in criminal acts, which makes it important to secure this data.
  - **Ethical/equity concerns.** Equity population representativeness within the training data set determines the generalization power of an AI system. If an AI method employs data gathered in an inequitable manner, the model and its decisions will be biased and will have the potential to harm misrepresented groups. Thus data equity focuses on acquiring, processing, analyzing, and disseminating data from an equitable viewpoint, in addition to recognizing that biased data and models can perpetuate

preconceptions, worsen racial bias, or hinder social justice. It is essential to check how those decisions are made and ensure that both the models and the data are free from any biases or mistakes.

- **Intellectual property.** This term refers to the ownership of inventions that can have commercial worth and legal protection. Such protection aims to ensure that the advantages generated from the exploitation of an idea or product benefit society and the inventor. Individuals and institutions with intellectual property have the right to bar others from using their inventions, having a direct and significant influence on their use or sale.

Trends

A multicloud, multifaceted operating model must also consider the following trends:

- Payers are implementing solutions that can support today's needs while also being future focused and integrating with solutions that providers eventually choose, instead of the other way around.
- Payers have eliminated data walls. Interoperability is mandated, and the need for SDOH, equity, census, and care data has opened data architectures to include many data sources and potential business partners. It is no longer adequate to only consider data within the enterprise.
- Payers and providers are working together in "payvider" models in which:
  - Healthcare providers are creating their own insurance plans.
  - Payers and providers are joining forces, including Aurora and Anthem (Well Priority), Banner Health and Aetna (Banner|Aetna), Cleveland Clinic + Oscar, MVP Health Care, and the University of Vermont Health Network.
  - An insurance company is shifting to being a healthcare provider that offers insurance. For example, Humana has announced its strategic shift from "an insurance company with elements of healthcare" to "a healthcare company with elements of insurance."
- Intelligent automation unifies artificial intelligence, robotic process automation (RPA), and patient engagement technology to perform common, repetitive, manual tasks the same way a human would.
- Artificial intelligence is determining when and how to perform workflows.

Conclusion

Establishing an overall vision of where the cloud enterprise approach is going and then modularly implementing sections of the architecture seems to be the most appropriate strategy. Retracting from the "cloud everywhere, cloud now" mindset is more effective and seems prudent. Restart now, and execute in a modular fashion toward an enterprise operating model that optimizes consistency, flexibility, and cost.

About the Analyst

Jeff Rivkin, *Research Director, Payer IT Strategies*

Jeff Rivkin is research director of Payer IT Strategies for IDC Health Insights. In that role, he is responsible for research coverage on payer business and technology priorities; constituent and consumer engagement strategies; technology and business implications for consumer engagement; front-, middle-, and back-office functions; value-based reimbursement; risk; and quality-based payment and incentive programs, among other trends and technologies that are important to the payer community.

MESSAGE FROM THE SPONSOR

Pure Storage accelerates the performance of core payer applications while protecting data assets and patient information.

By redefining the storage experience, Pure Storage simplifies how payer organizations consume and interact with data. Pure powers claims processing, medical management, back-office systems, and data-protection protocols with storage that transforms data into value. Storage as you need it is the Pure way, whether it's on premises, in the cloud, a hybrid model, or as a service. No more "click and wait" for answers. No more disruptive data storage upgrades. Just quicker insights for better patient care.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com