IDC

Unlock Innovation in Healthcare:

Unify and Simplify to Make Way for Intelligent Process Automation

RESEARCH BY:

Cynthia Burghard
Research Director, Value-based Healthcare IT
Transformation Strategies, IDC

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

Executive Summary

The demand on healthcare organizations to provide access to high-quality, cost-effective healthcare has never been greater, and yet the fragmented IT environment that contributes to operational inefficiency, redundancy, manual procedures, and data silos remains unchanged. Data is rapidly becoming the currency in healthcare, and yet less than 50% of organizations do not have a data management and governance structure. Data is inaccessible, holding back both analytic and artificial intelligence and machine learning (AI/ML) initiatives and efforts to automate business and IT processes. Most organizations decentralize their IT staff based on applications or functions. What is required is a unified platform.

A unified platform is at the center of the IT architecture. For the purposes of this document, it is defined as a "composable fabric" (everything as code) of related technologies that share a common framework for development, operations, and security using a standard-based approach for interoperability. The need is to centralize the pipeline for CI/CD (or CICD) so that all initiatives are subject to the same development and operation activities and teams by enforcing automation in building, testing, and deploying all applications. Most IT environments have multiple application types, including commercial off the shelf, AI/ML, and business process and data management that are not subject to consistent, standard processes and so result in long delays in delivery and significant manual effort.

Without unification and simplification of IT, healthcare organizations will continue to be challenged to deliver innovation and will be unable to take advantage of intelligent process automation (IPA) at scale.

Data is rapidly becoming the currency in healthcare, and yet less than 50% of organizations do not have a data management and governance structure.

State of the Healthcare Industry

Industry Demands

The healthcare industry is pursuing the quadruple aim: improve the health of the population, enhance the patient experience, reduce costs, and improve the work life of clinicians (**digital.ahrq.gov/acts/quadruple-aim**). These goals cannot be met with the current IT environment. These demands, coupled with the growing appetite for AI/ML for predictive analytics and intelligent process automation, require a simplified and unified operational and IT infrastructure.

Cost and Quality of Healthcare

The U.S. healthcare system continues to deliver poor financial and clinical outcomes despite efforts to "fix the system." Healthcare costs are growing nearly 1% faster than the gross domestic product (GDP), with estimates that they will make up 20% of GDP by 2028.[1] Further:

▶ The average deductibles in employer plans have more than doubled between 2008 and 2017, from $869 to $1,808 per year.[2]

▶ Only 62% of adults are very or somewhat confident in their ability to afford healthcare.

By many standards that measure quality, the United States continues to do poorly:

▶ The rate of U.S. maternal mortality is 26/1,000; in comparable, in developed countries, the rate is 9/1,000.

▶ The overall age-adjusted mortality rate per 100,000 is 840 in the United States compared with an average of 690 in similar countries.[3]

Attempts to slow the cost curve and improve quality have had limited success. Two levers have been used: The first is shifting the financial burden to the individual in hopes of encouraging more cost-conscious decisions on where and when to seek care. For example, enrollment in high-deductible health plans has increased during the past five years, from 20% of covered workers in 2014 to 30% in 2019. Even with increased financial incentives, individuals lack sufficient information to make these decisions.[4]

The second lever is government and commercial insurers engaging providers in risk-based contracting where providers are financially rewarded for reaching established quality goals or penalized for not meeting goals. This approach is relatively new, and results are mixed. The Centers for Medicare and Medicaid sponsored 54 cost management programs — only five programs show measurable savings. According to the National Association of Accountable Care Organizations, only 52% of accountable care organizations (ACOs) earned shared savings in 2019.[5]

1. Centers for Medicare and Medicaid: *National Health Expenditure Study*
2. Source: *KFF's Employer Benefit Survey*, 2018–2019
3. Source: World Health Organization
4. Source: *KFF's Employer Benefit Survey*, 2018–2019
5. Seema Verma – former head of CMS

The Patient Experience and Physician Satisfaction

These two quadruple aim objectives — enhancing the patient experience and improving physician satisfaction — require a unified, simplified IT environment. Friction for patients when attempting to navigate the healthcare delivery or insurance claim processes is significant. Unlike other industries, healthcare remains dominated by manual processes and data fragmentation, which make even the simplest task such as making an appointment require multiple phone calls. Patients are looking for convenient, continuous, and personalized care. While a top priority for both payers and providers, there have been only marginal improvements in patient satisfaction. The patient experience relies on accurate, appropriate, and consistent communication with the patient, allowing them to digitally communicate with both payers and providers.[6]

The concerns for physician burnout, particularly due to the additional stress on all clinicians during the COVID-19 surges, drive the need to address physician satisfaction. For example, the burden of clinical documentation and other largely manual processes must be reduced. Clinical documentation and payer processes that govern payment are ripe for transformation. Improving clinical processes and improving physician satisfaction were among the top drivers for AI adoption for healthcare respondents of the IDC's *Industry AI Path Survey.*

The importance of both patient and physician experience and satisfaction is front and center for both payers and providers. Both require data and process changes across the fragmented IT landscape. Healthcare organizations will realize greater value of their AI investment if standards are in place for both data governance and management and a unified approach to technology management and development.

Fragmented and Siloed IT Environment

An Environment Characterized by Legacy Technology and Complex Processes

The healthcare IT environment can only be described as legacy. Mergers and acquisitions, increasingly complex payer benefit plans, and a risk-averse industry have left healthcare organizations with an aging IT infrastructure. The core applications that run the business for payers are their administrative applications (e.g., claims, enrollment, billing, provider management, and care management) and are typically "off the shelf" and customized to meet the needs of the organization. Most are program code based on business rules built with a monolithic architecture that requires manual updating, a process that takes days and weeks. In a highly regulated industry, the complexity and volume of rules make these legacy applications brittle and difficult to manage in an environment that requires agility and speed to market.

Both internal and external environmental factors have created the inefficiency and fragmentation that exist in most healthcare organizations. On the health payer side, the need to support multiple and increasingly diverse insurance and noninsurance products has led to a proliferation of core transaction systems that each have dedicated maintenance and development resources, different tools, and siloed data. On the provider side, the number of mergers and acquisitions and the degree of customization of core electronic medical record (EMR) systems create the same type of fragmented environment as payers.

6. Source: IDC's *Industry AI Path Survey,* May 2021

The core application portfolio of providers includes revenue cycle management and electronic health record systems. This legacy environment shares some of the challenges of those of the payer environment in terms of high volume and complexity of rules in a heavily regulated environment. Off-the-shelf applications are heavily customized as well. The need to protect personal health information and abide by the Health Insurance Portability and Accountability Act (HIPAA) regulations in the United States and other such regulations in other countries adds additional challenges for maintaining privacy and security of personal health information in a legacy and splintered IT environment.

Healthcare organizations' move to the cloud has lagged due to the slow migration of legacy applications and security hesitancy. However, recent data indicates that apprehension is lessening as healthcare providers take advantage of cloud offerings.

Healthcare organizations continue to move workloads to the cloud, typically a combination of private and public cloud. The recent IDC's *Industry CloudPath Survey,* May 2021, reveals that budget constraints were identified as the trigger event for cloud adoption by the greatest number of providers, followed by growth of data beyond current capacity and the need for functionality only found on the cloud.[7]

The Data Dilemma

IDC estimates that on average approximately 270GB of healthcare and life sciences data was created for every person in the world in 2020. The global healthcare and life sciences DataSphere industry vertical represented roughly 7.3% (29.1ZB) in 2020. Healthcare organizations are facing a data tsunami as data from remote devices and sensors grows and access to external data sources such as consumer, social determinants, and genomic and geospatial data explodes — means that strong data management and governance remain key.

The operational deployment of AI/ML, as it extends to issues of ethical use and development of trust in data governance, calls for AI-specific data governance and management. Yet IDC data indicates that only 53% of healthcare organizations have specific AI/ML data management and governance policy and procedures in place. The remaining organizations have either no or limited policy or procedure in place to govern AI/ML deployment.

Results of a recent IDC's *Industry AI Path Survey* find that key challenges for healthcare organizations to enable AI include insufficient volume of high-quality data. Recognizing the limitations of data silos, healthcare organizations are creating integrated data platforms as a key initiative to ensure they will get value and ROI from AI/ML investments.[8]

Data within a healthcare organization is fragmented by and within functional areas. As enterprises have grown through mergers and acquisitions, the data fragmentation issue has grown. Finding the "single source of truth" is often likened to finding a needle in a haystack. Vendors with analytic platforms have undertaken the task of creating integrated data stores to support business intelligence and analytics but are challenged to bring data together to support AI/ML. Issues of duplicate data, varying data formats, and limited access controls present an inefficient environment and one that is a barrier to becoming a data-driven organization where data is key to decision making.

This dysfunctional environment also results in unnecessary investment to meet external reporting requirements. Healthcare is heavily regulated and as such carries a tremendous burden for external reporting. Inaccurate results or delays in meeting reporting deadlines are routine.

7. Source: IDC's *Industry CloudPath Survey,* May 2021
8. Source: IDC's *Industry AI Path Survey,* May 2021

IT Organizational Challenges

While the cloud provides the opportunity to unify and simplify the IT infrastructure, operational improvements need to be addressed. In today's IT environment, not only are there technology silos but staffing and operational silos as well. De facto walls exist between applications where development and production have designated teams that differ by application. Best practices across teams are rarely shared; each team has their own approach and maintains their own rules. Security protocols may not be consistently applied across all levels of infrastructure and processes. There is a need to balance the benefit of centralization and standards with the unique attributes/characteristics of applications.

While IT fragmentation and siloed workforce and data continue, the impact on the business escalates. Operationally, the cost of maintaining so many disparate systems with no communication or common standards for operations thwarts efforts to improve efficiency and introduce AI/ML. This coupled with the increasing pressure to make system changes based on new federal mandates — especially challenging through COVID-19, state-specific requirements, not to mention the security exposure — creates the imperative for unifying and simplifying the IT environment. Maintaining the status quo is not financially sustainable nor is innovation possible.

Healthcare Marching Toward AI/ML Adoption

The healthcare industry is ripe for AI/ML adoption with its fragmented IT and data environments and the continued pressure to deliver high-quality care at an affordable price. The three drivers of AI/ML adoption are improvement in operational and clinical efficiencies, insights at scale, and improving the patient and provider experience. Particularly in the provider market, the early experience with AI/ML was often limited to academic clinical studies that were funded by external government or private organizations. This reduced the experience of providers to more scalable commercial use cases.

Improving back-office, administrative, and clinical processes through the application of AI/ML is a driver of AI/ML adoption as well. An environment heavily dependent on paper and manual processes, with fax machines being the primary communication channel between payers and providers, produces unnecessarily high levels of friction between organizations. The prior authorization process is ripe for intelligent process automation; 30% of respondents in IDC's *Industry AI Path Survey* from payer organizations indicated that they had AI/ML algorithms in place for prior authorization, with an additional 31% of organizations indicating deployment by year-end 2021. Another example where AI has been successful is in assisting in the coding of hierarchical clinical conditions (HCCs) in which algorithms can identify incomplete diagnostic coding that leads to underpayment for Medicare beneficiaries, if not included. Advancements in improving clinical processes have lagged due to physician hesitancy and concerns over the potential to do physical harm.

Healthcare organizations have been using AI/ML to deliver insights through predictive analytics for several years. The identification and prioritization of patients in need of services, patients who might be at risk for readmission, or those with declining health are all use cases healthcare organizations are familiar with and actively using. The evolution of value-based health contracts and the need to identify patients who would benefit from care management and how best to engage them in care have been among the primary use cases for AI/ML. The ability of AI/ML to ingest multiple data sources increases the precision of the insight delivering a more effective intervention, resulting in a better outcome.

Improving the patient and member experience and improving physician satisfaction are among the top drivers for AI/ML adoption. Healthcare organizations responding to IDC's *Industry AI Path Survey* indicated that improving the member and patient experiences was key driver of AI/ML, and further 62% of providers indicated an increased spending related to AI for patient experience, and 58% of payers indicated increased AI/ML spending for member experience.

Two applications of AI/ML that benefit patients and members as well as providers are: first, reducing the burden of interacting with healthcare organizations. For individuals, it is about clearly mapping out the healthcare journey, helping comply with health improvements through empathetic support and reminders. Second, for providers, it is reducing the friction with their documentation systems (EMR), serving up data at the point of care that is most relevant to caring for a patient. The recently enacted patient access rule of the 21st Century Cures Act enables individuals access to their health data in virtually any format that can be enabled by AI/ML.

Healthcare organizations have been "stuck" in the pilot testing mode for AI/ML and struggle with operationalizing algorithms.

Payers are ahead of providers in their approach to AI:[9]

▶ 23% of payers and 5% of providers characterize their AI approach as aligned with business goals and repeatedly producing new business value.

▶ 26% of providers and 2% of payers characterized their AI approach as including a few AI initiatives, and they are uncoordinated.

Both payers and providers (77%) rely more heavily on third-party vendors as their primary AI development approach:[10]

▶ 28% of providers rely more on internal build than payers with only 1% using internal resources as their primary deployment approach.

▶ 55% of payers indicate they are using existing third-party vendors while only 26% of providers are using existing third-party vendors.

These challenges can be mitigated by establishing an Open AI automation platform.

9. Source: IDC's *Industry CloudPath Survey*, May 2021
10. Source: IDC's *Industry AI Path Survey*, May 2021

AI/ML Maturity in Healthcare:

Payers are ahead of providers, with 79% of payers considered "advancing" in AI versus 53% of providers.

77% of payers and providers rely on third-party vendors as their primary AI development approach.

28% providers versus 1% of payers are internally developing AI.
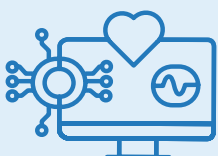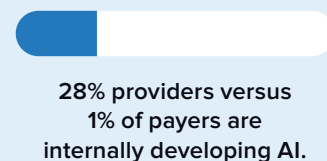
Healthcare organizations are ensuring value from their AI/ML investments by:
- Redesigning legacy process
- Evaluating use cases based on predicted value
- Using a common data integration platform for data extraction

Approach to Intelligent Process Automation for Healthcare

Intelligent process automation is the collection of technologies that come together to manage, automate, and integrate digital processes. The primary technologies that make up IPA include digital process automation (DPA), robotic process automation (RPA), and fields of AI such as computer vision AI and conversational AI and machine learning.

The objective of intelligent process automation is to reduce costs, generate revenue, and reduce risk.

Healthcare examples for these objectives include:

▶ **Reduce costs.** Identify that the variations in costs for the same surgery is due to the cost of a specific device, such as an artificial hip, and make recommendations for less expensive acceptable alternative. Improving operational efficiency in both clinical processes and in the back office is among the benefits healthcare organizations realize through AI.

▶ **Generate revenue.** Use ML and natural language processing (NLP) to review charts for accurate coding to improve HCC scores and reimbursement.

▶ **Reduce risk.** Predict risk of readmission and recommend a mitigation strategy to a care manager.

The pandemic provides a perfect example of the benefit of rapid response. Based on IDC surveys conducted throughout the course of the pandemic, we know that organizations with the ability to respond quickly to change are more resilient and are able to keep operations online. That was not the case in healthcare. Federal mandates that impacted payment for COVID-19 testing and treatment, for example, could not be implemented in a timely fashion by payers or providers. Making rule changes to payment and billing systems in healthcare takes weeks to complete, resulting in consumers receiving bills for services that should have been paid by insurance. In a unified and simplified IT environment, rule changes can be made quickly, consistently, and correctly with far less effort.

> **Based on IDC surveys conducted throughout the course of the pandemic, we know that organizations with the ability to respond quickly to change are more resilient and are able to keep operations online.**
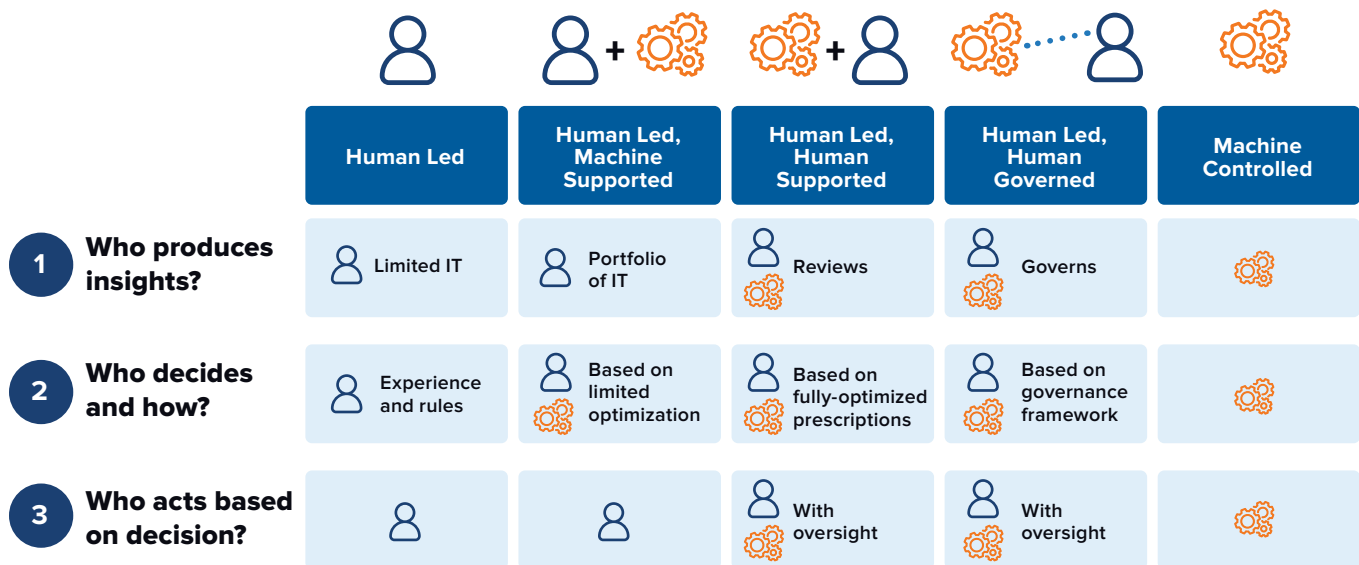
The IDC AI-Based Automation Framework

To help enterprises evaluate opportunities and mitigate risks of using AI for automation, IDC has developed the IDC AI-Based Automation Framework. Its intent is to guide business and IT leaders' AI technology decision making by defining expected degrees of AI-based automation evolution and the hierarchy of automation scope. The framework can serve as a basis for assessing data, algorithm, IT, and staffing requirements at the intersection of AI capabilities and use cases.

The IDC AI-Based Automation Framework has five levels (see **Figure 1**). To understand the likely evolution of AI-based automation, it's important to evaluate the interaction of humans and machines across these five levels and to understand who analyzes the data and who decides on the action based on the results of the analysis and determines who acts based on the decision.

FIGURE 1

The IDC AI-Based Automation Framework

		Human Led	Human Led, Machine Supported	Human Led, Human Supported	Human Led, Human Governed	Machine Controlled
1	Who produces insights?	Limited IT	Portfolio of IT	Reviews	Governs	
2	Who decides and how?	Experience and rules	Based on limited optimization	Based on fully-optimized prescriptions	Based on governance framework	
3	Who acts based on decision?			With oversight	With oversight	

At each level of automation, the following questions must be asked and answered:

▶ **Who produces insights?** Does the human or the machine (AI) analyze data and deliver insights from such analysis? Does the human or machine describe what something is, how it trends, why something is happening, and what might happen next? The result of the analysis or insight can vary widely based on the approach to producing the analysis. For example, the identification and stratification of patients in need of services can be generated by a human by using heuristics, rules, or AI predictive models. Each approach will deliver results, but the AI predictive model will use a greater variety of data and deliver more precise results.

▶ **Who decides and how?** Once all relevant analysis has been conducted, does the human or machine make the decision based on the derived insights? A decision can include a range of business/clinical or personal choices, such as a decision to recommend a care management program for patients based on their unique clinical, social, and mental health needs.

▶ **Who acts based on the decision?** Finally, should a decision lead to an action by either a human or a machine? The action can be in the digital or physical environment. The action is the execution of the decision and can include initiating a treatment based on AI-generated insights with or without consultation with a clinician.

While there is an increasing level of automation as we move toward the right side of the framework (refer back to **Figure 1**), the path is not always linear. It is possible that the machine-led, human-governed level may be followed by machine-led, human-supported level when variables such as data complexity or policies or regulations change. In other words, the path can be iterative. However, it is not enough to identify and define levels of AI-based automation. We must examine them also in the context of the scope of automation.

The AI/ML Automation Infrastructure

In addition to the IDC AI-Based Automation Framework as a tool for designing and managing AI automation in healthcare, it is critical to have the technology to operationalize AI/ML and other initiatives from development into production efficiently, timely, and error free. This unified platform contains all the relevant data, tools, and processes in one place. It must be open and include the orchestrated use of a wide range of technologies through an ecosystem of partners.

Data Governance and Management

Complexity of healthcare data and concerns regarding ethical use of data require an explicit set of policy and procedures governing data management, access, and quality. Individual authority must be identified and held accountable:

▶ Over 35% of providers had 10+ data sources being used in their organizations.[11]

▶ Over 80% of data in healthcare is semistructured or unstructured.

▶ 50% of providers will increase their spend in external data.[12]

▶ 68% of providers ranked ethics considerations as very challenging in AI deployment.

11. Source: IDC *Health Insights' Business Intelligence Survey*, August 2021
12. Source: *Meeting the Healthcare Industry's Demand for External Data* (Data as a Service) (IDC #US46756420, August 2020)

Across all industries, AI is managed through centers of excellence (COEs) and, in some organizations, a combination of centers of excellence and business units:[13]

▶ 42% of organizations managing AI centrally through COEs

▶ 22% manage at the business unit level

▶ 18% manage as a spoke (business unit) and wheel (COEs)

▶ 18% manage independently at the business unit/functional area including payment, model building, and maintenance

The most sophisticated organizations have data management and governance structures that include policy and procedure as well as explicit accountability. A best practice includes corporate policies and procedures for data governance and management of all AI initiatives, the chief data officer or individual in equivalent position is accountable, and the documents are reviewed and updated on a regular basis.

Many data management functions include individuals monitoring data quality and remediating "bad data" across the data supply chain, integrating data using interoperability standards, developing and managing role-based access to data, and protecting personal health information and other responsibilities. In some instances, these staff provide guidance and/or develop analytic applications including providing resources necessary to develop and deploy artificial intelligence.

The responsibilities include the creation and management of a central or single path from development to production. In today's environment, healthcare organizations have separate DevSecOps processes and teams for different applications. For example, there are likely to be different teams and processes for each of the multiple core administrative applications in a payer portfolio. Without centralization, each of those core administrative applications will have to make any rule change in each application. Centralization allows organizations to make one change and share it across the portfolio.

The IT Requirements

A unified platform is at the center of the IT architecture. For the purposes of this document, it is defined as a "composable fabric" (everything as code) of related technologies that share a common framework for development, operations, and security using a standards-based approach for interoperability. The need is to centralize the pipeline for CI/CD (or CICD) so that all initiatives are subject to the same development and operation activities and teams by enforcing automation in building, testing, and deploying all applications. Most IT environments have multiple application types including commercial off the shelf, AI/ML, and business process and data management that are not subject to consistent, standard processes and so result in long delays in delivery and significant manual effort.

The platform has three aspects or dimensions: infrastructure, data, and security. Together, the dimensions perform various functions across an open architecture, with an orchestration layer that moves data and processes when and where they are needed. It is not just about technology, it is about managed services, particularly in areas such as AI, as healthcare organizations often have limited access to data scientists. The legacy organizational and technical environment lacks

13. Source: IDC's *Industry AI Path Survey,* May 2021

discipline in areas of data management and governance that compound the need for centralization and active oversights.

Infrastructure

The purpose of the infrastructure domain is to simplify and unify the IT environment. The fragmented nature of healthcare IT results in data fragmentation, which coupled with the fragmentation of IT operations and staffing, continues to hold back healthcare organizations. Through acquisition and mergers as well as adding new businesses, the healthcare environment can be described as hyper-heterogeneous. For example, a payer may have separate claims processing engines to run each of their lines of business (e.g., commercial, Medicare Advantage, and Managed Medicaid), all of which share processing rules and have unique rules. Medicaid for example, varies by state.

In today's environment, each of the processing engines are supported by separate teams. When rule changes occur (a situation that happens frequently), each team makes changes to "their" rule, tests it, and then puts it into production. With each team having their own process for development and production, the change process can take several days or weeks. In a unified environment, changes can be shared and made in hours.

While the cloud environment provides a storage and compute environment to enable unification, there are other considerations for intelligent automation. Unifying the data is the first step toward intelligent automation. Intelligent automation supports the automation of tasks, activities, and processes. In the IT environment, this will include areas such as security and management of tasks, activities, and/or processes of the production environment. Healthcare is rapidly moving workloads outside its four walls while retaining some data internally on premises. Data will reside anywhere, and it must be accessible regardless of format, location, or latency (i.e., streaming, batch).

Moving workloads to the cloud does not resolve the underlying issues of lack of centralized approaches and management of development and production environments. The misconception that the cloud was just to store data and exaggerated benefits of the cloud left many healthcare organizations with unmet expectations. The cloud includes software as a service and platform as a service in addition to infrastructure as a service. These capabilities enable improved efficiency and faster time to value for developers.
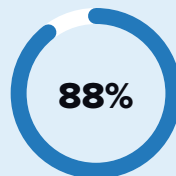
According to IDC's *Industry CloudPath Survey*, May 2021:
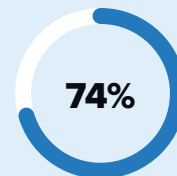
96%
of healthcare organizations are using the public cloud for two or more workloads.
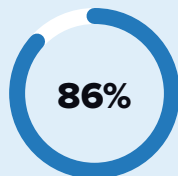
86%
of healthcare organizations are using a private cloud for two or more workloads.

88%
of healthcare organizations have or will have within the next 12 months workloads at the edge.

74%
of healthcare organizations have or will have within the next 12 months AI/ML workloads.

Data

The concept of a data supply chain where data is accepted and integrated from both internal and external sources, harmonized and normalized, and made compliant to internal and external security controls and accessible to deliver insights at scale and for all back-office and front-office applications is the objective.

Healthcare organizations recently reported that two strategies they use to ensure value from their AI investments are:

▶ 49% use/plan to use common data integration platforms to help extract data.

▶ 43% understand clearly what type and quality of data is needed to define and train models.

And yet when asked about barriers to AI development and adoption:

▶ 60% reported lack of adequate volumes of quality training data

▶ 57% reported operationalization of AI frameworks/libraries[14]

Value enablement strategies for AI and AI barriers can be addressed with the right infrastructure that harnesses data and provides access to data for intelligent automation in either back-office or clinical processes using AI/ML as well as other tools such as business rules management systems.

Data proliferation requires interoperability and strong data governance and management. Healthcare has long struggled with interoperability due to the lack of standardized adoption of data structures and meaning. The Interoperability and Patient Access final rule (CMS-9115-F) provides the impetus to improve interoperability. It gives patients access to their health information when they need it and in a way they can best use it. This final rule focuses on driving interoperability and patient access to health information by liberating patient data using CMS authority to regulate Medicare Advantage (MA), Medicaid, Children's Health Insurance Program (CHIP), and Qualified Health Plan (QHP) issuers on the Federally facilitated Exchanges (FFEs). This mandate has gone into effect for both payers and providers and above all else is intended to promote data exchange and access.

Data is the new currency of healthcare; organizations need to reduce the burden of data preparation so organizations can use data to improve decision making, improve clinical and back-office efficiency, deliver clinical best practices, and allow clinicians to practice at the top of their license. Some high-value use cases are:

▶ Reducing the friction between payers and providers by automating heavy manual processes such as preauthorization

▶ Improving the clinician's work experience by reducing documentation burdens

▶ Assisting with the diagnosis and treatment of illness

▶ Identifying fraud, waste, and abuse

▶ Improving patient compliance to care plan

▶ Providing image analyses

14. Source: IDC's *Industry AI Path Survey,* May 2021

Security

Healthcare organizations have overcome their early concerns about security and are embracing the cloud as a secure environment for their workloads and data. Whether due to breaches or the recognition that external third-party vendors have greater resources to ensure the safety and security of an organization's data and workloads, healthcare organizations are moving to the cloud.

The regulations protecting patient privacy in the United States through HIPAA and GDPR in the regions require rigid and consistently applied security to protect personal health information and to avoid data breaches that result in penalties. Data breaches are not uncommon. Data breaches are on the rise; the Department of Health and Human Services reported that there were 642 data breaches of more than 500 patient records in 2020 in the United States. In 2010, there were 199 data breaches of more than 500 patient records. Healthcare organizations are slowly trusting the cloud as a secure environment as breaches within their IT organizations continue. In a recent survey, 29% of healthcare organizations identified improved IT security as one of the benefits of moving to the cloud. 37% of healthcare organizations identified "keeping up with compliance across regions (GDPR, etc.)" as a trigger event for cloud adoption.

Simply putting data and workloads on the cloud does not ensure security; a unifying platform as previously discussed where security is part of the entire instance (for example, by deploying DevSecOps) and not applied piecemeal as an afterthought must be a security consideration to consider. The automation of security protocols to detect when systems are out of compliance with HIPAA and initiate changes to bring the system back into compliance can be applied to protect the entire IT environment.

While the cloud is providing a "secure" environment, healthcare organizations must recognize that data is located across many locations and security must be consistently applied across all environments.

Data breaches are on the rise; the Department of Health and Human Services reported that there were 642 data breaches of more than 500 patient records in 2020 in the United States.

Essential Guidance

It is critical for healthcare organizations to better understand the barriers to innovation and scaling intelligent process automation. Data fragmentation, legacy technology, and decentralized IT operations and staffing are well-known challenges, but the response of many healthcare organizations continues to be tactical. There has never been a time of greater pressure for healthcare organizations to use information to drive business and automate the low-value, repetitive tasks that are prone to error and cause both cognitive and time burden on staff. To move forward healthcare organizations must:

▶ Establish an organizational vision with requirements and metrics for a unified and simplified environment for intelligent process automation. Define success in measurable terms and a time frame for meeting interim and final goals.

▶ Use the three pillar platform identified previously (IT infrastructure, data, and security) to build your organization's vision and strategy.

▶ Identify members of the executive leadership who will evangelize the introduction of intelligent process automation. They must open the doors, quell the fears, and celebrate the successes.

▶ Evaluate tasks, processes, and even systems that would benefit from intelligent process automation.

▶ Identify those automation opportunities that both yield visible benefits and cause the least disruption to operations or threaten the current culture.

▶ Determine the appropriate level of automation through the application of the IDC AI-Based Automation Framework in terms of level of comfort with machine-led activities.

▶ Do not underestimate the level of change management that will be necessary for even the "least threatening intelligent automation" initiatives.

▶ The pressure for healthcare organizations to meet the demands of consumers, clinicians, and regulators has never been greater. Tactical initiatives will not meet these demands; a unified and simplified approach to manage data and its use across the organization are what is needed to move the healthcare industry forward.

About the Analyst

Cynthia Burghard
Research Director, Value-based Healthcare IT Transformation Strategies, IDC

Cynthia Burghard is a Research Director with IDC Health Insights where she is responsible for the value-based healthcare practice. A key focus of her research includes the use of cognitive/AI technologies to advance digital transformation in healthcare. Areas of research include analytics, population health workflow, proactive patient engagement including patient personal assistants.

More about Cynthia Burghard

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC   ◢ @idc   in @idc   idc.com