cloudticity

Migrating Epic EHR to AWS

Typical challenges and what you can do now to overcome them

Table of Contents

Taking On The Challenge

Significant numbers of hospitals and other healthcare organizations are migrating their Epic environments to the public cloud. They make this decision seeking to minimize capital investment, scale quickly and easily, make developers more productive, and most importantly, drive improvements in the customer experience (learn more here).

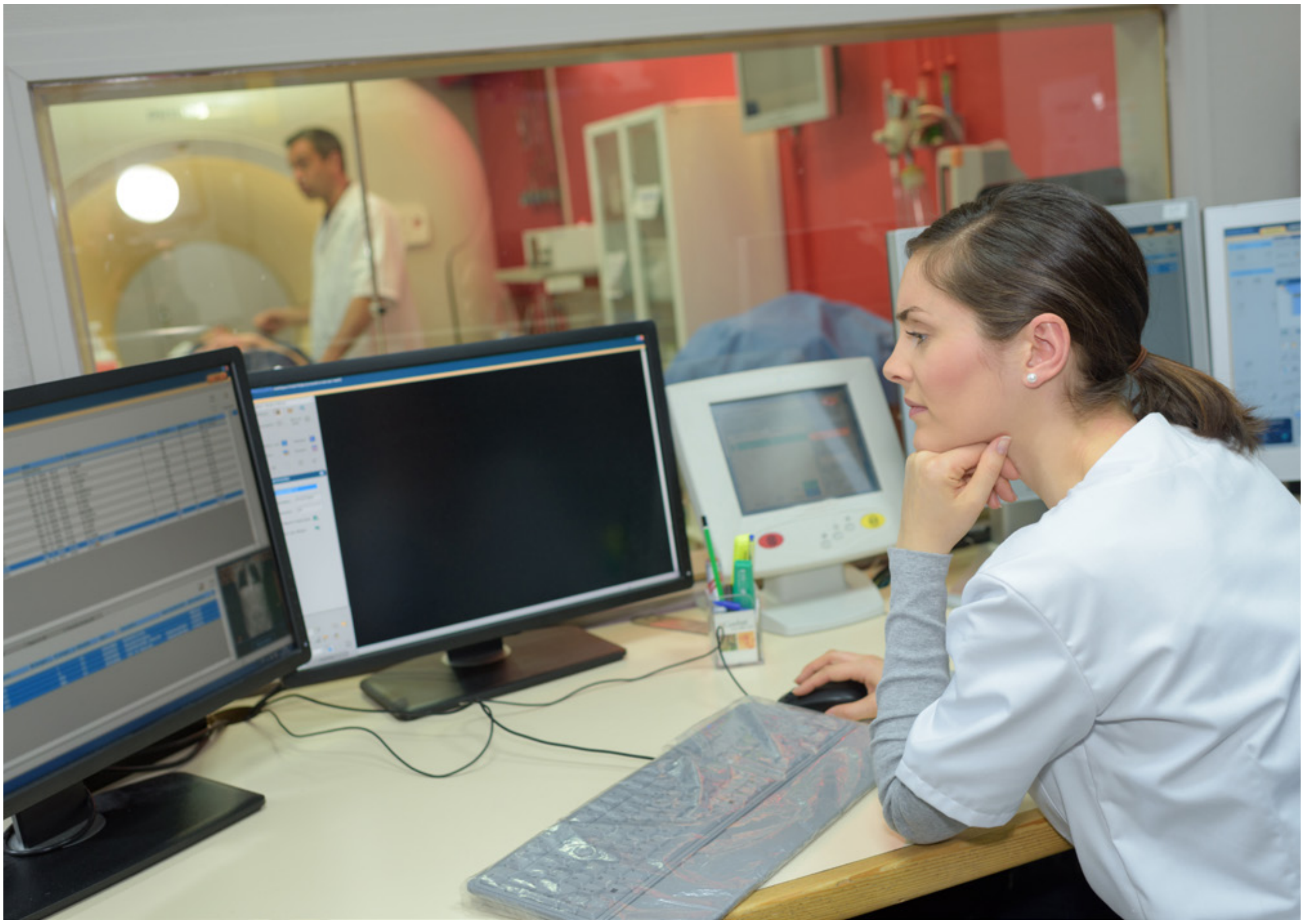
Given the importance of Epic to their operations, healthcare IT leaders need to conduct due diligence investigations to ensure that moving Epic to the cloud is the best choice for their needs. This white paper is intended to help IT decision-makers understand the breadth of challenges involved with an Epic migration to public cloud provider Amazon Web Services (AWS). Most of this information applies in general to other public cloud providers as well.

First, it presents background information about public clouds in general and AWS services in particular. Then the paper lays out some architectural information to provide more context for technical readers. The following two sections outline the technical and business challenges, respectively, that organizations are likely to face in designing their migration.

The final section makes the case for engaging a managed services provider (MSP) early in the process. One of the potential pitfalls of an Epic migration is making critical decisions serially without realizing the impact that early choices have on other aspects of the deployment. It is imperative that healthcare IT leaders have a clear picture of the end state of the migration and the steps involved in reaching that destination before they start on the journey. They need someone who has been there and done that. That's what Cloudticity has to offer.

Cloud Basics

This section provides background information on public cloud, virtual public clouds, and cloud services — key concepts that apply to any migration to the cloud.



Public Cloud Models

Public cloud is actually an umbrella term that covers three primary business models for delivering services. You will often see the notation XaaS, which stands for Software/Platform/Infrastructure As A Service.

Software as a Service (SaaS)

In the SaaS model, a third party manages the application and the infrastructure — the entire stack (see figure 1). SaaS requires very little technical support within your organization — the SaaS provider handles everything. While SaaS is technically a public cloud service, the migration from on-premises applications to SaaS is fairly straightforward and is not discussed further here.

Typical SaaS providers: Microsoft Office 365, Google Workspace (Docs, Slides, Sheets), Salesforce.com, SAP and NetSuite.

Platform as a Service (PaaS)

PaaS is a framework for developers to create customized applications. In a PaaS model, the provider provides the hardware, operating system, and runtime environment, while your organization manages the applications and data. This cloud model is also beyond the scope of this paper.

Typical PaaS providers: Typical PaaS services include AWS Elastic Beanstalk, Heroku, Windows Azure, Force.com, Google App Engine, and OpenShift.

Infrastructure as a Service (IaaS)

Conceptually, IaaS is essentially a data center run by someone else who charges you for the resources you consume. With IaaS, you run your application on the provider's infrastructure, relieving your organization of the cost and complexity of building and operating a data center. Of the three models, IaaS is the one that involves the most involvement by your organization. When this paper talks about cloud, it means IaaS unless otherwise noted.

Typical IaaS providers: AWS, Microsoft Azure, Google Cloud Platform, and Alibaba. There are also niche IaaS providers that focus on specific industries. The rest of this paper is concerned only with IaaS unless otherwise specified.

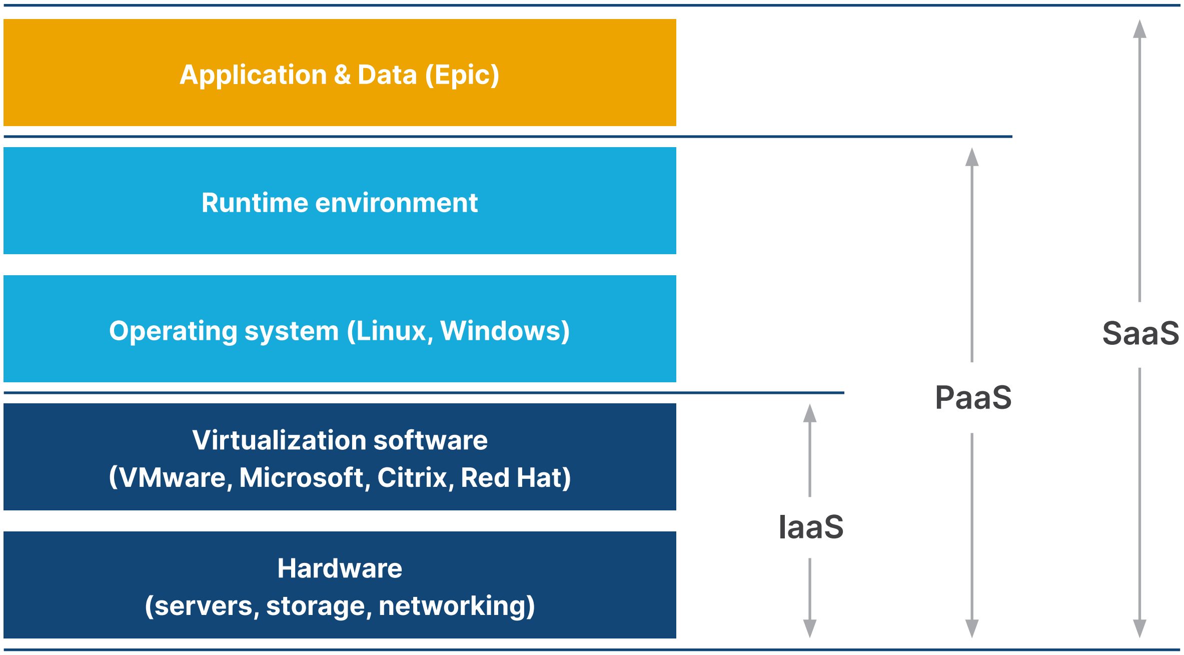

Application & Data (Epic)
Runtime environment
Operating system (Linux, Windows)
Virtualization software
(VMware, Microsoft, Citrix, Red Hat)
Hardware
(servers, storage, networking)
IaaS
PaaS
SaaS

Figure 1. IaaS, PaaS, and SaaS Vendors' Areas of Responsibility

Cloud Services

IaaS usually consists of computing, storage, and networking resources, but for today's public cloud providers, infrastructure has a far broader meaning. AWS offers more than 200 pretested services that can dramatically shorten development times and improve the quality of cloud-based applications. More than 120 of these services are certified to be HIPAA eligible (see figure 2).

The building-block appearance of these services can be deceiving because, for the most part, they are far from plug and play. Creating a web application using AWS services requires careful architectural design, deep knowledge of how the services work, and a lot of custom connective tissue—the kind of knowledge that only comes with experience using these services. With Epic deployments, the system designer must also understand the constraints of the various regulations that govern healthcare IT. For these reasons, most healthcare organizations seek design assistance from an MSP with a strong practice in healthcare.

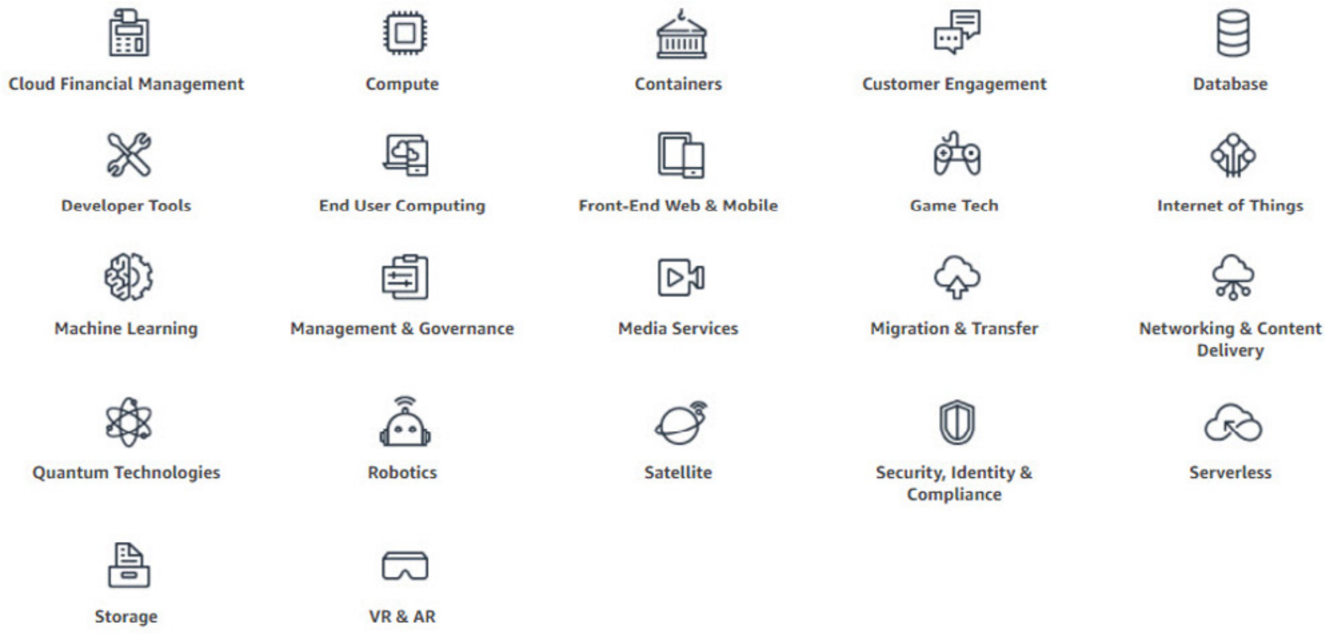


Figure 2. Categories of AWS Cloud Services

Virtual Private Clouds (VPCs)

A key concept in public cloud deployments is the virtual private cloud (VPC)[1]. In a sense, VPCs give you a way to have it both ways in the cloud world, offering the scalability and convenience of public clouds combined with the data isolation of private clouds. In a nutshell, a VPC is just a private cloud that runs on a public cloud. The public cloud vendor ensures the VPC is truly isolated from everything else on the same infrastructure using a range of security technologies (see table 1).

One obvious question is, why not just use a private cloud? Scalability is one advantage. For all practical purposes, public clouds have infinite amounts of computing, storage, and network resources. In addition, self-service portals can deploy these resources in minutes.

VPCs also offer better security, because public cloud providers invest heavily in security infrastructure to avoid a breach that could strip off billions of dollars of market capitalization in a single day. The infrastructure of a public cloud is highly likely to offer better security than anything your organization can implement and operate.

VPCs extend your geographic reach to the points of presence (PoPs) of the cloud provider all around the world. This capability is especially helpful for low-latency applications for which performance suffers from too much latency. In essence, you can locate key applications and data locally while maintaining centralized control and governance.

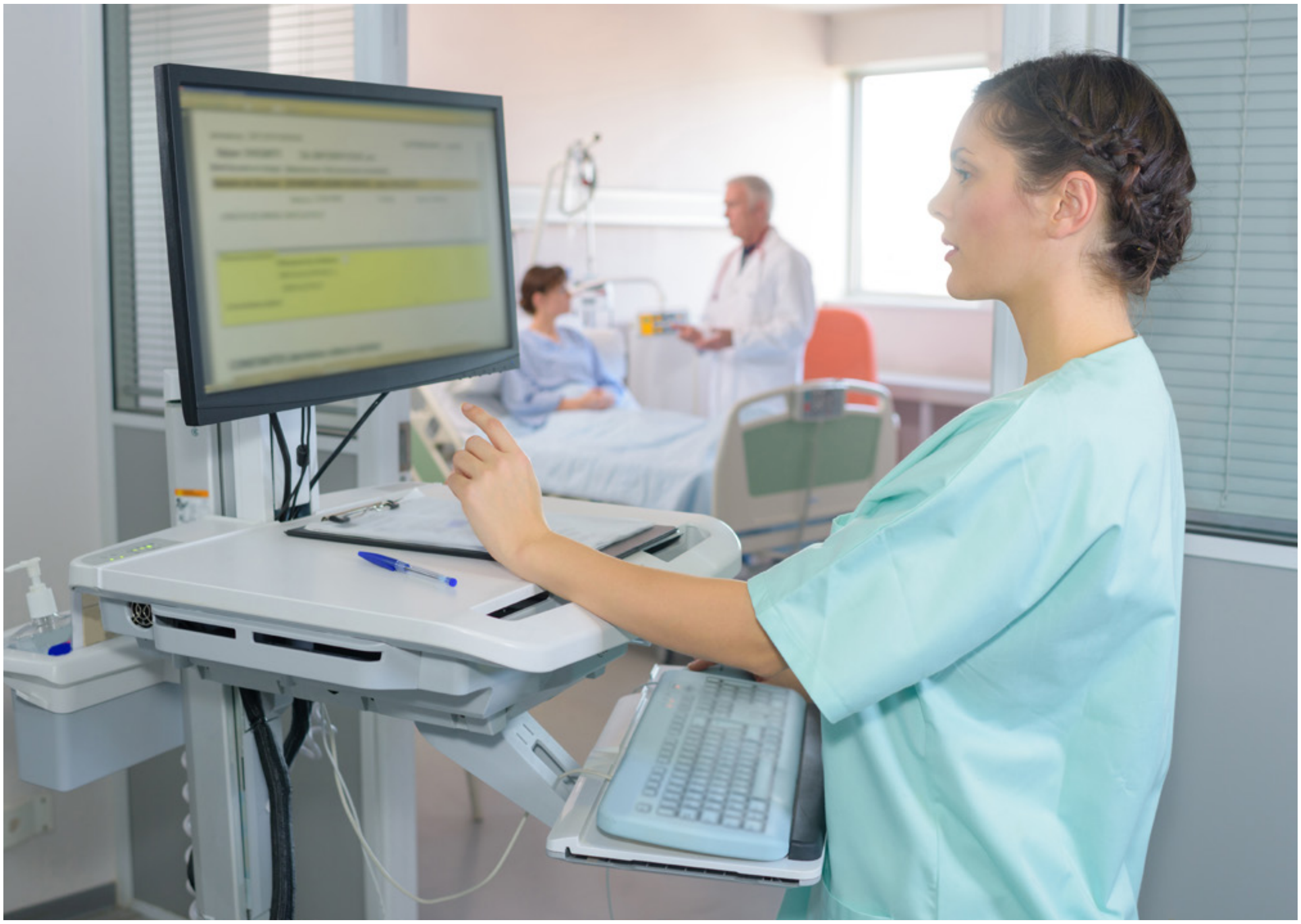
[1] https://www.cloudflare.com/learning/cloud/what-is-a-virtual-private-cloud/

Table 1. Security Technologies for Isolating VPCs

TECHNOLOGY	DESCRIPTION	PURPOSE
Subnets	Range of IP addresses within a network that are reserved for the VPC only and not visible or accessible via the internet.	Prevent would-be attackers from finding IP addresses, a first step to many attacks. In a VPC these are private IP addresses that are not accessible via the public Internet, unlike typical IP addresses, which are publicly visible.
VLAN	Local area network (LANs) that groups together servers and other devices that are not physically connected.	Provide a similar level of protection as subnets but works at Layer 2 instead of Layer 3 (subnets).
Virtual private network (VPN)	Private network that uses encryption to run over the internet.	Foils attempt to steal data—even if the attacker gains the transmission, encryption renders it useless.
Network address translation (NAT)	Method for matching private IP addresses to a public IP address visible on the internet.	Allow public-facing websites or applications to run securely inside a VPC.
Border gateway protocol (BGP)	Primary signaling mechanism on the internet.	Customize BGP routing tables for connecting VPCs with other parts of the infrastructure (requires substantial knowledge of network technology to use properly).

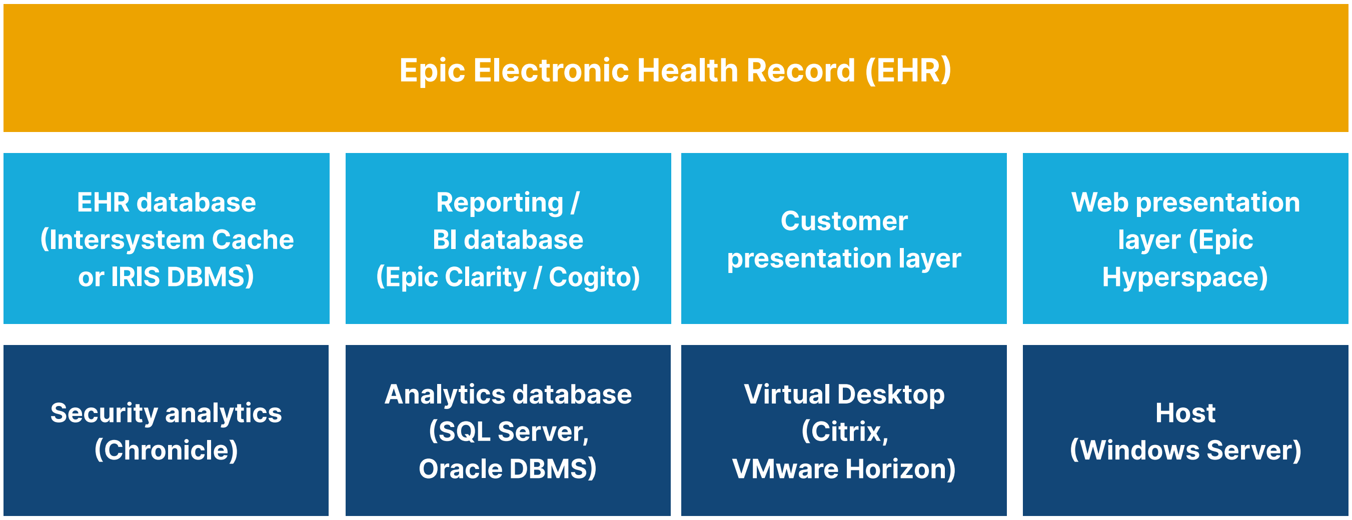
Epic on AWS Architecture

This section provides a more technical overview of key components of a complete Epic deployment in the cloud, including the Epic EHR, the Epic core VPC, the test/dev/training VPC, and the disaster recovery VPC.



Epic Electronic Health Record (EHR)

The Epic EHR is built on four technology pillars: EHR database, BI/reporting database, customer presentation layer, and web presentation layer (see figure 3)[2].



Epic Electronic Health Record (EHR)

EHR database (Intersystem Cache or IRIS DBMS)

Reporting / BI database (Epic Clarity / Cogito)

Customer presentation layer

Web presentation layer (Epic Hyperspace)

Security analytics (Chronicle)

Analytics database (SQL Server, Oracle DBMS)

Virtual Desktop (Citrix, VMware Horizon)

Host (Windows Server)

Figure 3. Technology Pillars of the Epic EHR

[2] Epic on AWS Technical Guide

Epic Core Virtual Private Cloud (VPC)

You can think of the Epic Core Virtual Cloud (VPC) as the heart of the Epic environment, the place where the EHR information resides, as well as critical functions such as email and access management. The architecture is built for redundancy, with two availability zones. Availability zones are a mechanism to partition the Epic Core environment to achieve high availability. Each availability zone runs on its own physically distinct, independent infrastructure with independent power, cooling, network, and security.

Within the VPC, components are placed in security groups, which are highly dynamic, software-defined micro-perimeters to control both north-south and east-west traffic. Rules determine which security groups can talk to each other. AWS components such as EC2 instances, S3 storage buckets, and database servers can belong to more than one security group (see figure 4).

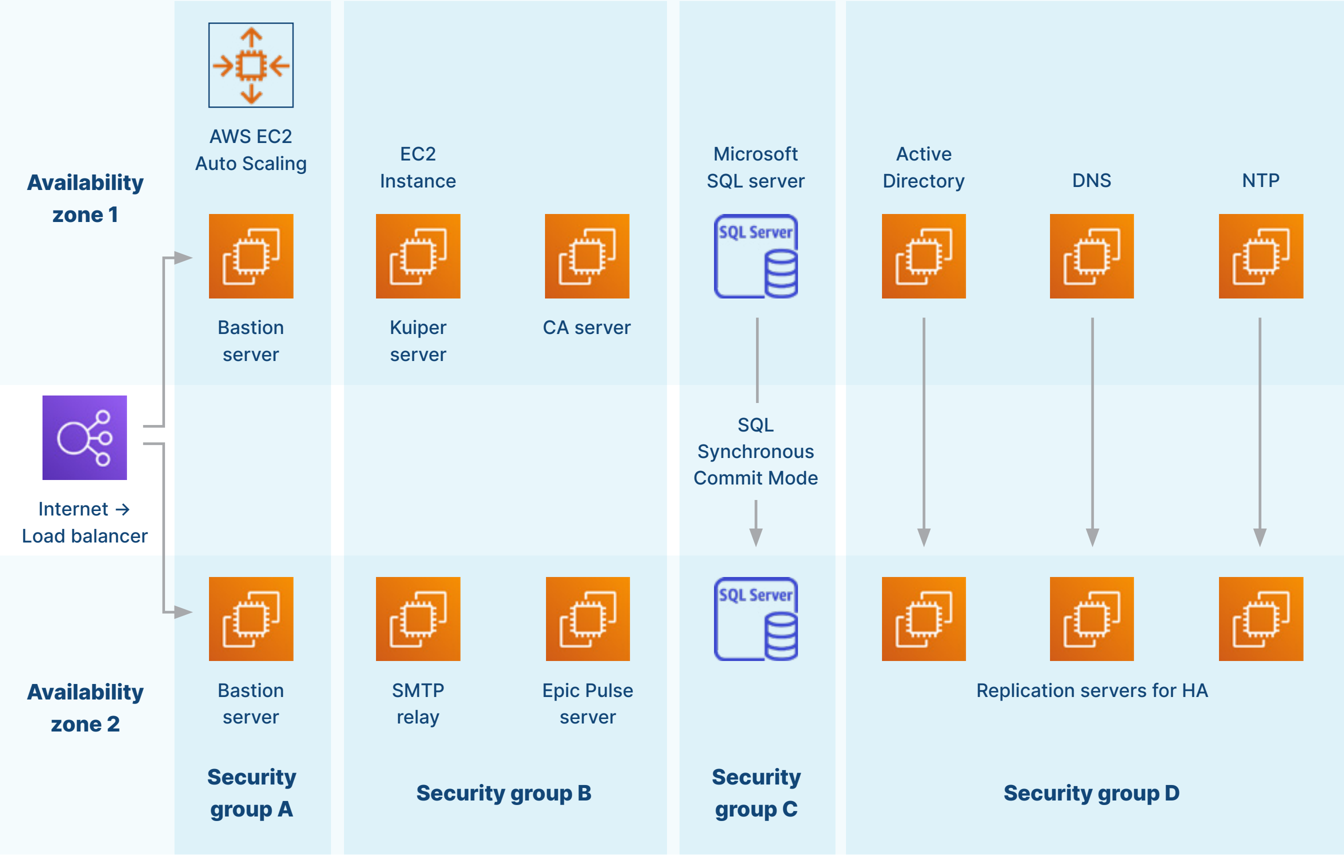


Figure 4. Critical Components of the Epic Core VPC

The icon identified as "EC2 instance" refers to the basic computing building block for AWS environments. An AWS EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the AWS infrastructure. Amazon provides a variety of types of EC2 instances with different configurations of CPU, memory, storage, and networking resources.

AWS EC2 Auto Scaling service helps you maintain application availability and allows you to add or remove EC2 instances automatically using dynamic and predictive scaling. Dynamic scaling responds to changing demand and predictive scaling automatically schedules the right number of EC2 instances based on predicted demand. You can use dynamic scaling and predictive scaling together to scale faster.

Epic System Pulse is the primary tool for monitoring applications in the Epic environment by consolidating information from various resources into a single data repository.

Kuiper is a tool used to install, support, and maintain the Epic client software, including Hyperspace, Epic Print Service (EPS), Business Continuity Access (BCA) devices, Web BLOB (WBS), Hyperspace Web, Interconnect, and System Pulse.

Microsoft SQL Server is the relational database used in the Epic core VPC for logging and management purposes. Information in this database is replicated in a second instance of SQL server using SQL synchronous-commit mode (more on SQL Server availability modes here).

Replication servers mirror critical information for redundancy and reliability purposes.

Test/Dev/Training VPC

Most healthcare IT departments segregate test, development, and training functions from the more mission-critical production workloads. In the public cloud, this separation is achieved by situating test/dev/training in its own VPC. Many Epic migration plans take advantage of this consideration by starting with the test/dev/training VPC as the first stage in the migration. This approach has clear advantages:

Risk reduction

You can build a complete test/dev/training environment in AWS, run all the necessary testing to ensure that it meets the design specifications, and then switch developers, test engineers, and training specialists over to the new environment in a phased approach. The legacy test/dev/training environment remains fully operational until all users have made the transition successfully, avoiding interruptions and productivity losses.

IT skill building

Healthcare CIOs can use the construction of the test/dev/training VPC as a learning platform for the internal staff to come up to speed. Working side by side with the MSP or third-party consultant, IT engineers can gain familiarity with AWS and public cloud technology far better than with classroom training (although there is often a need for formal coursework as well).

Cost and time savings

The ease of spinning up new development, testing, and training environments is a revelation to most users. They like the fact that they can engage the resources they need without having to navigate the formal IT process for procuring and installing new hardware and software. Furthermore, the resources can be decommissioned when the need is satisfied, avoiding paying for computing, storage, and networking functions that are not being used. Any CFO who has chafed at the sight of a full rack of servers sitting idle between training sessions can appreciate the value of on-demand resourcing.

User advocacy

Developers are known to be picky about their working environments, so winning them over to a cloud-based deployment can go a long way to creating a favorable impression of the benefits of moving Epic to the cloud. In some cases, early adopters become raving fans who act as ambassadors to others in the organization who are reluctant to migrate Epic to the public cloud.

However, there is a caveat: The ease with which non-IT people can consume cloud resources means that costs can mount up if environments are not properly decommissioned. Internal governance is required to achieve the full potential cost savings of using on-demand resources.

Disaster Recovery VPC

If you think CFOs worry about a few training servers that are underutilized, imagine how they feel about an entire backup and disaster recovery (BDR) site. There is no question about the need — HIPAA compliance requires that hospitals and other healthcare organizations have three plans in place:

- **Data backup plan:** Procedures to create and maintain retrievable exact copies of electronic protected health information
- **Emergency-mode operation plan:** Procedures to enable continuation of critical business processes for the protection of the security of ePHI while operating in emergency mode
- **Disaster recovery plan:** Procedures to restore any loss of HIPAA-protected data

The good news is that implementing a disaster recovery plan on AWS has significant advantages over traditional environments. When you move BDR to the cloud, you essentially trade the fixed capital expense of a physical backup data center for the variable operating expense of a rightsized environment in the cloud. This can significantly reduce total cost of ownership. You can take advantage of the AWS CloudEndure service for data replication or use your own BDR application.

An AWS-hosted BDR VPC is far less complex and easier to manage because AWS provides the hardware and software resources. Testing is easier to conduct in the public cloud, allowing your IT staff to test more frequently and build confidence in your ability to recover to your stated targets. Finally, the highly automated nature of AWS-based disaster recovery decreases the chances of human error and improves recovery time.

As with the test/dev/training VPC, you can bring up the BDR VPC in parallel with your existing site and even run them together until you are convinced that the cloud-based BDR VPC meets your requirements. For many organizations, BDR constitutes a good choice for proof-of-concept initiatives.

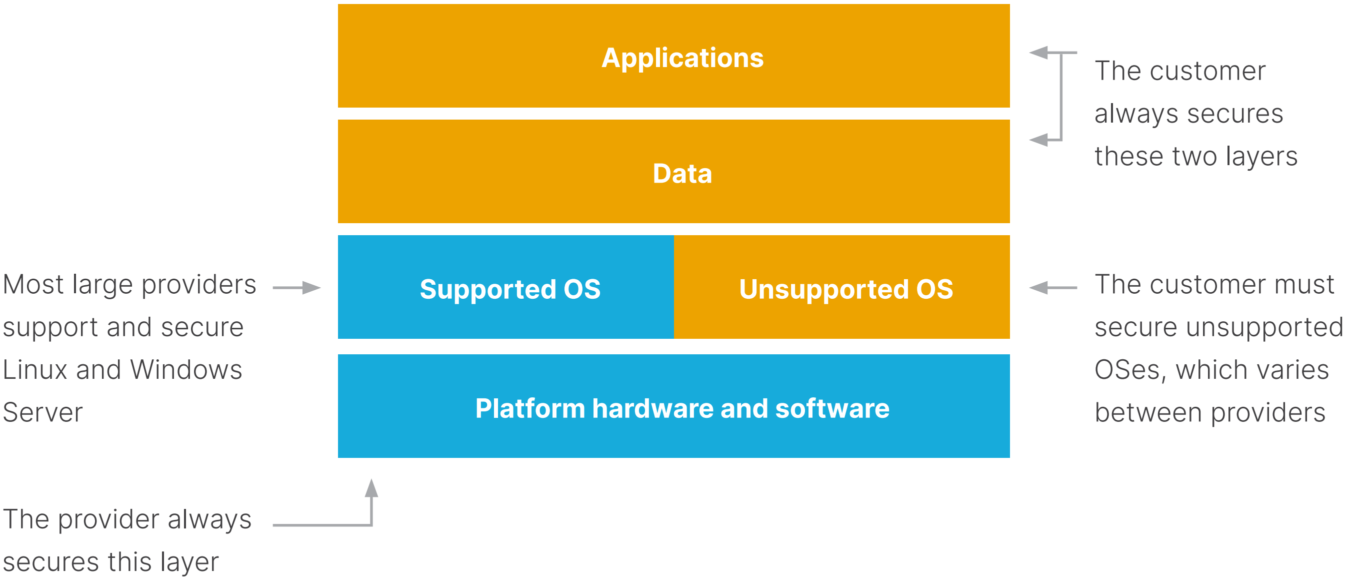
Technical Challenges

As you plan your Epic migration to the cloud, you will encounter several technical challenges. Here are some key areas where you can expect to devote significant effort to educate you and your staff as to the best way to overcome these obstacles.

Sharing Is Caring:
Security in the Public Cloud

Security is handled differently in the public cloud, so it’s important to design your security strategy with these differences in mind. As is the case with all public cloud providers, AWS secures the platform —that is, the hardware and software that power the cloud — and, in most cases, the operating system too. Securing applications and data (valuables) is your responsibility (see figure 5).

However, AWS also offers services you can use to build your security infrastructure. These optional services address areas such as data protection, threat detection, identity and access management, compliance and data privacy, and application protection. Learn more here.



The customer always secures these two layers

Most large providers support and secure Linux and Windows Server

The customer must secure unsupported OSes, which varies between providers

The provider always secures this layer

Figure 5. Shared Security Responsibility in the Public Cloud

Talk To Me:
The Need for Interoperability

Interoperability of health information is key to effective care delivery in today's diverse healthcare ecosystems. To take a recent example, the lack of space for therapeutic equipment forced many hospitals to transfer COVID-19 patients, requiring a swift and accurate transfer of medical records as well.

The big EHR vendors all claim to support interoperability, but challenges remain. Broadly speaking, there are three primary obstacles to seamless interoperability:

- **Inconsistent coding.** There is no consistent way of identifying a patient across the healthcare spectrum. The most common identifying data are name, date of birth, and Social Security number. However, this information can be coded in different ways in different systems leading to patient identification errors.
- **Lack of messaging standards.** Several standards development organizations have led collaborative processes with healthcare IT users to develop proposed standards, but there is no single agreed-upon standard for information exchange. Seemingly trivial differences such as mismatched fonts or custom data fields can require that information be manipulated and sanitized before it can be imported into another system.
- **Information Blocking.** While there are regular calls from industry groups and government agencies to end the practice, some EHR vendors continue to block certain kinds of information that they consider proprietary or charge a fee for transmitting the data outside the system.

Two Efforts to Standardize Health Data Sharing

- CommonWell, an alliance formed six years ago, operates a health data sharing network that enables interoperability using a suite of services aiming to simplify cross-vendor nationwide data exchange.
- Carequality, a recent initiative of The Sequoia Project, is a national-level, consensus-built, common interoperability framework to enable exchange between and among health data sharing networks. Nearly all major EHR vendors have aligned with at least one of these efforts.[3]

All that said, Epic has a relatively good reputation for interoperability due to its range of tools for sharing data (see table 2). According to a recent study, Epic Systems is the first vendor to make real progress toward universal patient data sharing and interoperability.

> **Most Epic users reported access to outside data and nearly two-thirds say they have achieved deep interoperability.[4]**

[3] https://www.hcinnovationgroup.com/interoperability-hie/interoperability/news/21162439/klas-epic-cerner-nextgen-stand-out-in-latest-interoperability-report

[4] https://ehrintelligence.com/news/epic-systems-tops-major-ehr-vendors-in-health-it-interoperability

Table 2. Epic Interoperability Between Health Systems

TYPE	DESCRIPTION	EPIC TECHNOLOGY
Shared instance	Organizations using Epic can share the patient’s EHR with other providers in the community.	Community Connect
Web portal	Community providers can access the patient chart via a web portal, so that they can follow the patient's care across the health system, schedule appointments, place orders, and more.	Care Link
EHR request (Pull)	A health system using Epic,can send out requests to other health systems. The external systems send information in the standardized summary (C-CDA), which can then be incorporated with the patient's local record.	Care Everywhere
Direct messaging (Push)	The organization that is currently seeing the patient can send the standardized C-CDA summary to another organization. This method is most commonly used for referrals.	Care Link

Security Holes in the Cloud:

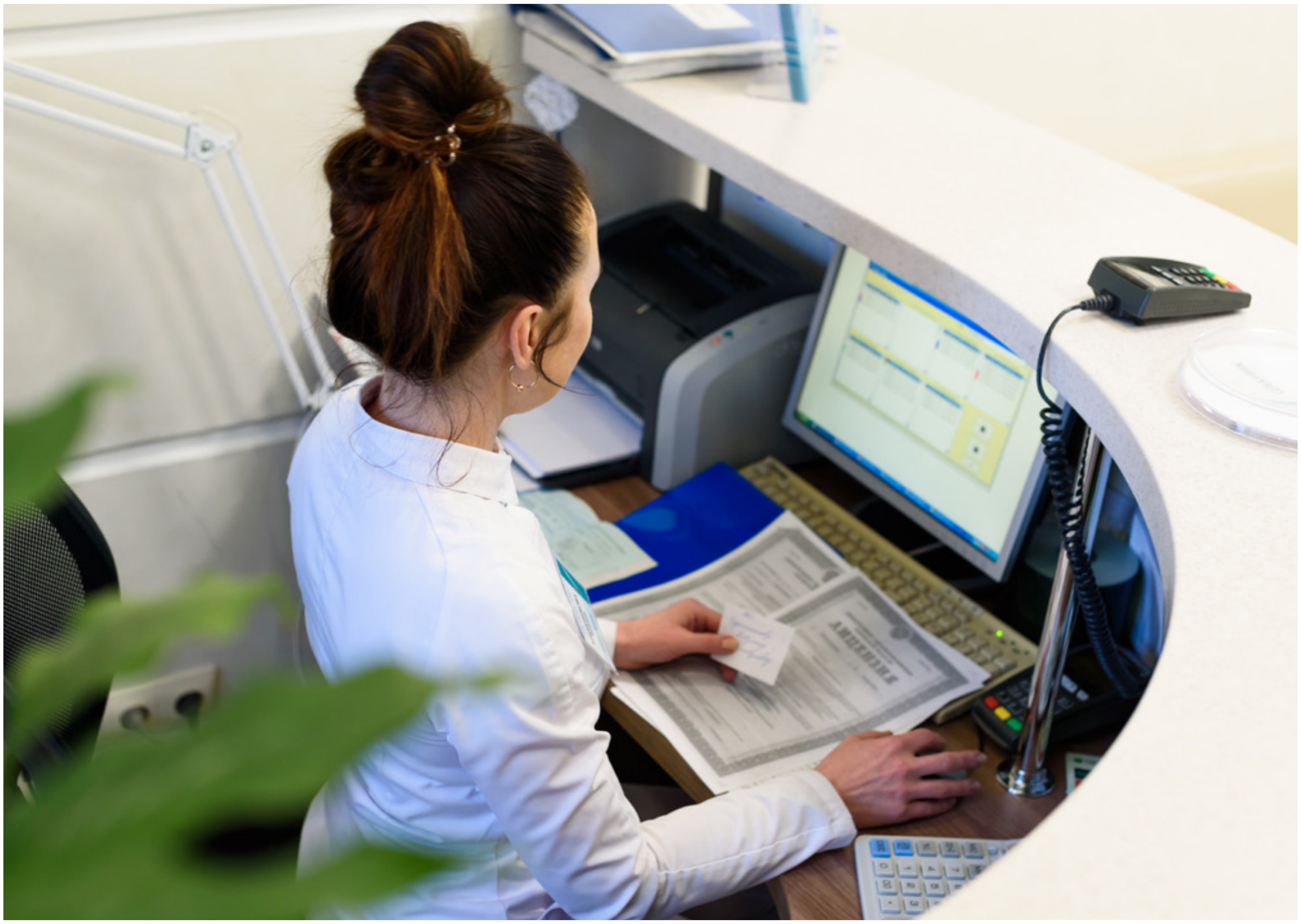
Shadow IT

To a hospital CIO, shadow IT is as scary as it sounds. Shadow IT refers to the practice of bypassing IT rules and regulations about cloud usage and instead creating your own account — in effect, going rogue. Shadow IT can be quite the temptation; after all, anyone with a company credit card can start spinning up computing and storage resources completely unknown to anyone else in the organization. Developers are perhaps the worst offenders because they are frequently under pressure to deliver working code; they may simply take matters into their own hands when local server resources are busy or not working.

Shadow IT can run up your cloud costs substantially, create holes in your security perimeter, and compromise compliance with HIPAA and other regulations.

Management Challenges

In selling the concept of an Epic migration to the cloud, you will encounter challenges on the business side too. Here are some of the more common ones.



A Little Help, Please:
Bridging the Skills Gap

Healthcare companies are scrambling to cope with a shortage of health IT professionals. A recent survey by the College of Health Information Management Executives (CHIME) found that 67 percent of healthcare providers are experiencing IT staff shortages.[5] The shortage in skills is impacting the way CIOs run their departments, forcing them to recruit highly specialized staff who have in-depth knowledge of the cloud and EHRs.[6]

The good news is that most healthcare IT professionals can come up to speed on the basic knowledge they need to manage a public cloud Epic deployment with some outside help. When selecting an MSP or other third-party, look for one that puts an emphasis on knowledge transfer and collaborative work from the very start.

Cloudticity has had outstanding success using the “shoulder to shoulder” approach in which the organization’s healthcare IT staff are paired with MSP experts and obtain hands-on experience all along the way. Beware of vendors who want to do it all for you — that’s rarely a good deal no matter what they charge; it can lock you into a costly arrangement that compromises your ability to manage your outsourcing spend and respond to changes in the marketplace.

[5] https://healthcareglobal.com/hospitals/bridging-healthcare-it-skills-gap

[6] https://healthcareglobal.com/hospitals/bridging-healthcare-it-skills-gap

Not In My IT Infrastructure:
Overcoming Cultural Resistance

Migrating to the cloud is a disruptive event, so it’s no surprise that many organizations encounter resistance from their staffers. However, the real work of overcoming resistance starts at the top. Senior management in general — not just the CIO organization — must understand the reasons for moving Epic to the public cloud and the benefits they can expect to see. Therefore, the Epic migration leadership team must invest considerable time educating executives to build a coalition of support and enthusiasm for the migration.

With buy-in achieved at the top, the next step is engaging the people who will be directly affected by the change. Experience has shown that mandates from senior leaders are not effective; in fact, they can engender even more resistance. Instead, bring them on the journey through open forums where they can express concerns and receive informative and supportive answers. Providing training early in the process sends the message that you value your staff and are willing to invest in their success. If you adopt this approach, don’t be surprised to find that some of the most resistant employees become evangelists, which can greatly increase the prospects of a successful transition.

I Thought Cloud Was Cheaper:

Managing Expenses

Migrating your applications to the cloud usually has cost benefits eventually, but early in the process, costs can actually go up for a variety of reasons.

For one thing, AWS deployments must be expertly tuned to ensure that resources are allocated and deallocated effectively, avoiding the case where unused instances remain provisioned and thus incur charges. Data transfers are another potential pitfall, because some cloud providers charge a per-gigabit fee when you move data out of the cloud. Therefore, applications that move large volumes of data between your data center and the cloud can drive up your cloud bill substantially. Applications that sync data between cloud and local data centers are particularly susceptible to this situation. Before finalizing on a cloud migration, you would do well to consult with a knowledgeable MSP who can help you navigate the different pricing options offered by the provider and fine tune your usage to keep costs down.

In the end, managing your cloud spend comes down to financial governance. Make sure that your MSP advises you on options such as chargeback, in which usage charges are allocated to the departments using the resources and thus catch the attention of budget-conscious department managers.

Fly Me to the Moon:
Setting Expectations

Perhaps the biggest potential pitfall on the business side of the house is unrealistic expectations. Promising too much and delivering too little is a recipe for ongoing scepticism in the executive ranks and sluggish adoption of new ways of doing things by the rank and file.

To avoid this hazard, think big and start small. Present the big picture of a cloud-based future Epic and then propose to execute a relatively limited proof-of-concept (POC) project — migrating one of the Epic test/dev/training environments is often a good place to start. Develop ways to communicate progress on the POC and setbacks to senior staff using dashboards and summaries that offer at-a-glance information about the trial project. Find an enthusiastic executive sponsor who can both advise and advocate at the highest level. Managing expectations may not be the most fun part of the job, but it can very well spell the difference between success and failure.

Four Things You Can Do Now

It pays to prepare your organization for the migration well before you solidify the plans. Engaging key employees in the process early sends the message that you value your existing staff enough to invest in them and their careers. In addition, the more your IT team knows about the environment to which Epic EHR is moving, the more they can help in the planning and implementation stages.

1. Assess Your Internal Skills

Perform a thorough assessment of your IT team's experience and expertise and rate their skills level (high, medium, low) in eight key areas[7]:

- Database technology, especially query languages such as SQL and the Apache Hadoop ecosystem
- Programming languages and environments such as Node.js, Java, and .NET
- Linux and Windows operating systems
- Networking
- Web services such as REST, XML, SOAP, UDDI, and WSDL
- Application programming interfaces (APIs)
- Cloud security
- Public cloud providers such as AWS, Microsoft Azure, and Google Cloud

[7] https://biztechcollege.com/technology/skills-for-cloud-computing-career/

2. Mitigate Skills Gaps

Once you have identified the areas where your internal team lacks the necessary skills, triage the skills into three categories: Train, Hire, or Outsource. This categorization is fluid and will change over time depending on your migration plan and choice of outside resources such as MSPs. Here are some strategies to consider:

- Define a set of basic skills that all IT staffers need—for example, Linux, database, networking, and security—and develop a training plan. Even if you plan to outsource or hire specialists, having a baseline knowledge within the group is vital.
- Identify top performers in your current staff and offer them third-party certification programs. For example, a network certification such as Cisco Certified Network Associate Cloud (CCNA Cloud) not only benefits the organization but can be a valuable career asset.
- Hire a specialist with cloud EHR experience. No matter how much you train your staff, there is no substitute for having at least one person with hands-on experience managing an EHR implementation in the cloud. The concepts of running EHR in the cloud are similar among EHR vendors, so it is unnecessary to find someone with Epic experience.
- Use your gap assessment to inform your requirements for third-party help. MSPs vary widely in their focus and expertise. Many CIOs put a strong emphasis on finding an MSP with strong expertise and experience in cloud security for healthcare due to the stringent regulations governing hospitals and other healthcare organizations.

3. Audit Your Data Privacy Strategy

When planning a migration to the cloud, many healthcare organizations are surprised to find that they have PHI scattered all over the organization, often with inadequate data privacy protection. An Epic migration provides an opportunity to institute more stringent controls for data privacy. Typical strategies include encrypting PHI at rest and in transit, preventing PHI downloads to USB sticks and other portable storage devices, protecting PHI on internal systems with firewalls, and restricting access to EHRs to authorized individuals.

A recommended practice is to engage a qualified MSP or other third party to perform a security risk assessment (SRA) of your current environment. SRAs identify, assess, and implement key security controls in applications.

Carrying out a risk assessment shows you how your application portfolio appears to a prospective attacker. It's important to do it before planning the migration to avoid replicating poor data privacy practices in the new environment.

4. Engage Outside Resources

A common mistake that healthcare organizations make is to wait too long to bring in outside help. The recommended time to engage an MSP or other third party is before the decision to migrate is finalized. Internal discussions about the pros and cons of migrating help your MSP understand not only the project requirements, but the thinking behind them. The more you think of your MSP as a partner rather than just another vendor, the greater the likelihood of a successful migration.

To help you decide, here is a checklist of the minimum set of attributes you should look for in an MSP.

Dedicated healthcare practice

Only an MSP with a strong practice in healthcare can fully understand your goals and challenges. Be wary of those who brush off the importance of industry-specific knowledge—healthcare is unlike any other industry, and the last thing you need is an MSP learning on the job.

Security experience

Among the unique challenges of moving from on-premises Epic to Epic in the cloud, cloud security is the most complex and critical. The ideal MSP has multiple case studies showing how they have secured healthcare organizations similar to yours and the benefits that those clients achieved. Make your security evaluation based on evidence, not a sales pitch.

Automation and AI

The MSP business model is undergoing a major shift, from people-intensive to automation and artificial intelligence. Watch out for MSPs that rely exclusively on human monitoring and manual remediation. Today's cloud-based Epic deployments are far too time-critical for human response times—threat remediation needs to happen in seconds to prevent damage from fast-moving exploits such as ransomware. While human expertise is always necessary, reliance on people rather than automation is a risky strategy.

Cultural match

Your chosen MSP will be a partner throughout the Epic migration and beyond, so their culture must be compatible with your own company's culture. In particular, pay attention to values. How transparent are they in terms of costs and timelines? How well do they listen and internalize what you're saying? Do they ask the right questions? What impression do your key people have of the MSP staff with which they have contact? Do they just rubber stamp your requirements or do they challenge them to make sure you have it right?

Although it may seem counterintuitive, application-specific knowledge of Epic EHR is not a requirement for an MSP. The reason is that the MSP works at the infrastructure level to ensure that the application functions just as it did in an on-premises deployment.

Put another way, the Epic migration is a success when Epic users are unaware that anything has changed. Your MSP will count on you to provide the application-specific knowledge needed to ensure a smooth migration while they focus on the infrastructure needs.

Why Cloudticity?

Once you've made the decision to move to the cloud, you will need expert assistance — Epic migration is not a job for the uninitiated. Consider Cloudticity as your MSP. Cloudticity is a digital enablement partner for the healthcare industry, generating measurable business and clinical outcomes by unlocking the full potential of the cloud. Through groundbreaking automation and deep cloud expertise, Cloudticity solutions empower healthcare organizations to create and scale the next generation of healthcare solutions. We have built some of the earliest and largest health systems on the cloud, including:

- The first patient portal.
- The first health information exchange (HIE).
- The first FISMA High deployment on AWS GovCloud.
- The first cloud-forward Meaningful Use 2 (MU2) compliance attestation for a large hospital system.
- The first COVID-19 registry on the public cloud for a state health department.

Cloudticity transforms healthcare IT into a driver of business and clinical value. For more information about how Cloudticity can help with your Epic migration to the public cloud, visit us here.

cloudticity

Start Your Journey to Business Value Today

SPEAK WITH A SPECIALIST