cloudticity

Five Things You Need to Get Right In Your Epic Cloud Migration

Table of Contents

IT'S "GO TIME"

Your healthcare organization has decided to migrate Epic to the public cloud – and you're leading the initiative. GIven the importance of Epic to the business, this assignment is make or break – your career, that is. You can be forgiven for being a little bit – or a lot – anxious about how you're going to pull it off.

This document can help. Cloudticity, along with our partner Sapphire Health Consulting, have put together this checklist of checklists to help you get the migration right, the first time. It is our sincere hope that this information is helpful and timely. We also hope that you will consider Cloudticity and Sapphire Health Consulting as partners in this important journey (more on us at the end of this document.)

Now, fasten your seatbelts and secure your tray tables.
We're about to launch you on your Epic migration.

ASSEMBLE THE RIGHT TEAM

An Epic migration is a lot like climbing Mount Everest. Both are difficult journeys that require specialized skills in a number of important areas and effective teamwork to reach the summit. Furthermore, failure is extremely costly — lost lives on Everest, derailed careers from botched Epic migrations. Remember, you can't build the climbing team on the slopes – the right personnel must be present and ready to roll before you leave base camp.

Inventory your internal resources

Epic migrations require expertise in areas that you almost certainly lack in your current organization. In addition, your staff is already busy keeping the lights on, so even when they have the right skills, they often can't be spared from what they're currently doing. Conduct a complete inventory of the certifications and experience of your IT staff. Review current and future initiatives to determine availability of key resources. The key skills needed for a successful Epic migration include:

- Cloud infrastructure (specific to your CSP)
- Epic technical infrastructure (ODBA, ECSA)
- App and Desktop Virtualization
- Operating systems (typically RHEL)
- Cloud security best practices
- Hybrid cloud networking
- Project management
- DevOps/cloud-native application development (nice to have)
- Data science/engineering (nice to have)

Fill skills gaps

The time to identify and fill skills gaps is before you start the project, ideally before the planning stage. In most cases, you'll need outside expertise in two specific areas: 1) the Epic platform itself, and 2) public cloud infrastructure. Be skeptical – make potential vendors prove convincingly that they have the experience, expertise, and track record of success to execute the specific responsibilities assigned to them.

Define roles and responsibilities

Never assume that people know who's doing what by their job titles, departmental names, or reputation. Assign primary and secondary responsibilities to each major area of expertise, for example, project staffing, management reporting, data security, infrastructure design, vendor coordination, and resourcing.

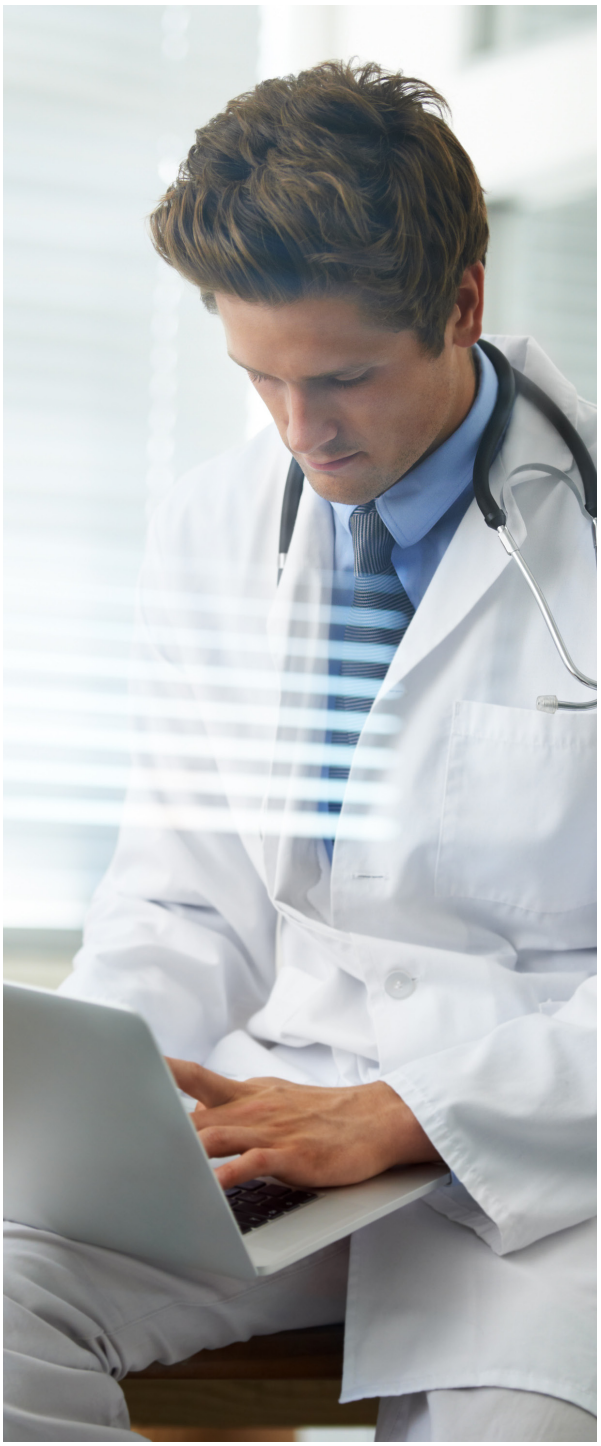
Strengthen executive sponsorship

You wouldn't be considering migrating Epic to the cloud unless the CEO, CFO, CIO, and CISO were firmly behind the plan. However, it pays to cultivate relationships with high-level stakeholders in the offices of the Chief Medical Officer, Chief Nursing Officer, Chief Medical Information Officer, Chief Compliance Officer, and others. During the lifecycle of the migration, issues will almost certainly come before the executive staff, and the more juice you have there, the better.

BUILD THE RIGHT MIGRATION PLAN

To paraphrase Mark Twain's famous quip about the weather, everybody talks about planning, but nobody ever does anything about it. While detailed planning for an Epic migration can be tedious when everyone is champing at the bit to get going, it's impossible to overemphasize the importance of having a detailed project plan.

One way to approach planning is to first paint a clear picture of the end state, that is, what your infrastructure will look like when the full migration is completed. Then work backward to identify intermediate stages at which specific capabilities have been transitioned to the new infrastructure, for example, backup and recovery. But however you do it, do it right.



Phase the project based on risk

There's nothing new about dividing a major project into phases, but how you divide up and prioritize your Epic migration can make the difference between success and failure. Lean toward migrating smaller, more discrete, non-production chunks of the platform first as a way to mitigate risk. Many organizations start with either of these areas:

- Non-PRD (Training): A non production environment such as a training environment is r==ical and business processes to switch over to the cloud. Designing your cloud-based BC/DR infrastructure gives your architects valuable experience working with the native services of your cloud provider and improves your chances for success when you tackle your migration of production capabilities.

- Backup and recovery: The business continuity infrastructure is largely separate from production, which means that you don't have to interrupt clinical and business processes to switch over to the cloud. Designing your cloud-based BC/DR infrastructure gives your architects valuable experience working with the native services of your cloud provider and improves your chances for success when you tackle your migration of production capabilities.

Socialize and propagate the draft plan

It would seem to be a given that anyone planning a major infrastructure project would circulate their draft plans widely for review, but that's not always the case. While it can be annoying and distracting to get critical feedback on your well-thought-out plan, the earlier you know about possible problems, the better. Furthermore, the socialization process is a way to get as many stakeholders as possible on board because they feel some ownership by virtue of having a say in the plan. Always make it a point to respond to every suggestion, even those you aren't planning to implement, to build trust and model transparency.

Plan for problems

If you've done careful and thorough planning and socialized the plan with the major stakeholders, what could possibly go wrong? A lot. The pressure to get the migration accomplished quickly can be enormous, but you won't get there faster with unrealistic expectations. A good rule of thumb is to build in 10%-15% slack in each major phase of the project and reevaluate at each major milestone. No one is going to be unhappy if you finish a task earlier than scheduled, but everyone will be unhappy if you fail to deliver on time.

Update the plan continually

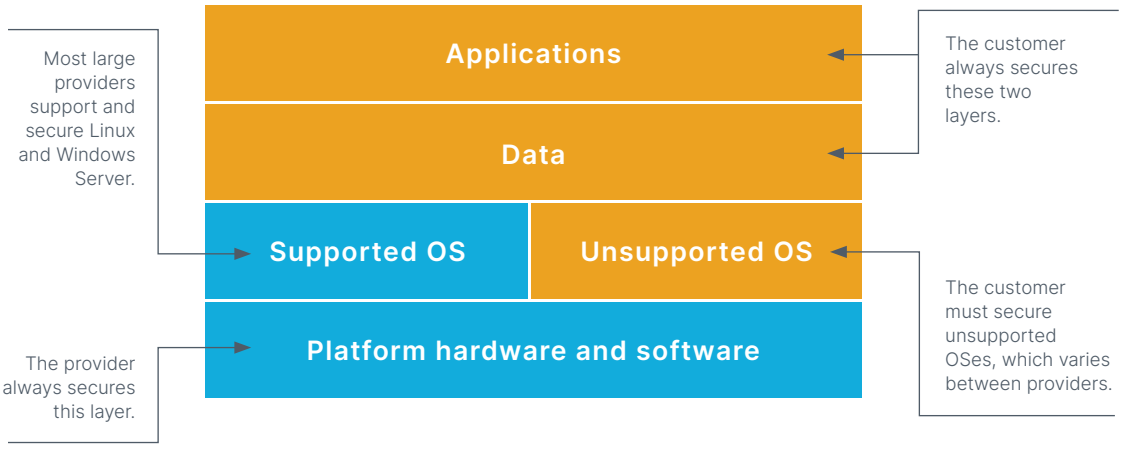
In many cases, project plans get pushed to the side once the work gets underway, but that can be a mistake. Having a formal process for updating and communicating plan revisions is essential for teamwork and transparency. Remember that new employees, contractors, and vendors will be coming on board during the course of a long migration project and they will need to rely on your planning documents to come up to speed rapidly.

EMPLOY THE RIGHT DATA PROTECTION

Data in motion is data at risk – the likelihood of data loss or corruption is highest during the time when information is physically moving from your existing environment into the public cloud. While data migration may seem like a technology problem, it's really a business-critical risk mitigation project. Healthcare organizations have the responsibility to safeguard not only personal health information but also personal information such as banking information and credit card numbers that could be used for malicious purposes.

Public cloud providers employ the principle of shared security responsibility in which the provider is responsible for the security of the platform – hardware and software – while the customer must ensure the security of the applications and data that reside on the platform. As with any divided responsibility, this seemingly neat and tidy model is prone to gaps which create vulnerabilities that cyberattackers are all too quick to exploit.

Shared Security Responsibility in the Public Cloud



Lock down your access control process

Your Epic migration will involve new categories of privileged users such as cloud architects, site reliability engineers and DevOps engineers. Your security staff must exercise strong oversight of their access privileges using least privileges principles. Place time limits on access and make sure that participants who leave the project – planned or unplanned – have their access privileges revoked as quickly as possible.

Encrypt all information in transit

For most organizations, encryption for moving information is already standard security policy. However, the Epic migration takes place outside of your normal workflows, so don't assume that existing policies will automatically provide the required security. Your migration partners should have expertise in this area.

Understand cloud compliance

As a healthcare organization, you must comply with a wide range of regulations such as the Payment Card Industry Security Standards Council (PCI-ISS), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the General Data Protection Regulation (GDPR). However, when you migrate to the cloud, you have to depend on your CSP for compliance because they, not you, control the infrastructure. Fortunately, all the major CSPs have strong compliance programs including the ability to generate the reports you need for your regulatory audits. You can get CSP-specific information here for AWS, Azure, and Google Cloud.

TRACK THE RIGHT METRICS

It's a commonplace that you can't manage what you can't measure, and Epic migrations are no exception. Everyone in the loop, from the people in the trenches to the top execs, needs to know how the project is progressing – the good, the bad, and the ugly.

Migration KPIs

Three KPIs are important for ongoing tracking of the migration process: duration, cost, and disruption.

Task duration

The most basic unit of project tracking is the length of each task and phase in the migration. You created a project plan with milestones, so the logical thing is to measure predicted versus actual time span. Time overruns not only lead to increased costs and missed deadlines, but they can be leading indicators of faulty assumptions or underperforming resources in your project plan.

Running costs

You might be surprised at how often cost accounting for large projects is put off until the project is completed – do now, count later. That unfortunate practice robs project managers of valuable information that can help them avoid catastrophic overruns but also pinpoint problems in the migration before they show up in missed milestones. Labor costs constitute the lion's share of the costs associated with any large migration project, so it's vitally important to track resource usage accurately along the way.

Business disruption

The prime directive of any Epic migration should be to cause no disruption to the business. The level of business disruption can be monitored using metrics such as application availability, number of service tickets generated, and unplanned downtime. A good practice is to establish baselines before starting the Epic migration so you can filter out the routine noise and identify the impact of the migration project itself.

Post-Migration KPIs

Once the migration is complete, be sure to institute KPI tracking right away and compare port-migration performance to pre-migration numbers. The four key post-migration areas to measure are infrastructure performance, application health, user experience, and cost savings.

Infrastructure performance

Measure hardware and network usage using metrics such as CPU utilization, memory usage, disk performance, network latency, and load balancing. Most cloud implementations include a dashboard where you can see these and other metrics in real time. Remember that applications and services that are not cloud-native might not use resources as efficiently as they did when they were on-premises.

Application health

The ultimate measure of the success of your Epic migration is how well the Epic application itself performs. Leverage Epic's System Pulse to monitor your environment's performance. Nearly a third of businesses undergoing a cloud migration report issues with availability during the first year.

User experience

Assessing the user experience complements application health metrics and gives you a complete picture of the operational impact of the migration. Look for changes in areas such as response time, spikes in requests, and length of user sessions. In addition, formal or informal user surveys often show problems early, before the tickets start flooding in.

Cost/time savings

On the financial side of the house, it's all about return on investment (ROI). ROI isn't easy to measure accurately, but some helpful inputs include cloud provider monthly costs, ongoing staff costs, management time, and third-party invoices. The challenge in the calculation is that on-premise ROIs are dominated by the capital costs of hardware and software, which are negligible in cloud deployments where operating costs dominate the ledge. Nevertheless, decision-makers need an accurate comparison of the cost of running Epic in the cloud versus the legacy on-premise system to assess the success of the Epic migration.

CHOOSE THE RIGHT PARTNERS

After you have completed the Epic migration, the real work begins. Now you're in for the long haul of operating a completely re-architected Epic platform running in an unfamiliar public cloud environment. That reality poses questions such as:

- *Who is going to operate the platform?*
- *How are you going to troubleshoot problems?*
- *How can you monitor and defend against cyberthreats?*
- *How will you minimize operating costs?*
- *How do we handle upgrades and routine maintenance?*

The time to answer these questions is now –once you fire off the project, life will be coming at you fast. .For many organizations, the solution will be to outsource some or all of these task areas to qualified MSPs

Epic technical infrastructure

Setting up and maintaining the Epic system requires specialized knowledge of the Epic architecture and ancillary systems and tools as well as best practices to ensure optimum performance. In addition, Epic deployments are in practice whole ecosystems that encompass other healthcare providers, insurance companies, patients, and more. A managed services provider can be responsible for initiating and maintaining these connections, which lifts a substantial operation burden from your staff and keeps the ecosystem healthy.

Cloud security management

Unlike data center deployments that have a well-defined security perimeter, hybrid Epic architectures are essentially boundary-less because of the constant movement of data into and out of the cloud and the huge number of possible attack points. Also, the virtualized nature of cloud environments requires virtual firewalls, which are managed somewhat differently from their hardware cousins. The right managed security services provider (MSSP) can improve your security posture and reduce the burden on your IT staff.

CSP business model

Each of the primary cloud service providers – Amazon Web Services (AWS), Microsoft Azure, and Google Cloud – have their own business models and service offerings, which can be tricky to navigate. An MSP who knows your cloud service provider inside and out can add significant value by helping you choose the right pricing tiers to minimize your spending for computing, storage, and networking services. In addition, your MSP can help you configure and deploy tools offered by your cloud provider in areas such as security, analytics, compliance, configuration management, and AI/machine learning.

ABOUT CLOUDTICITY

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.

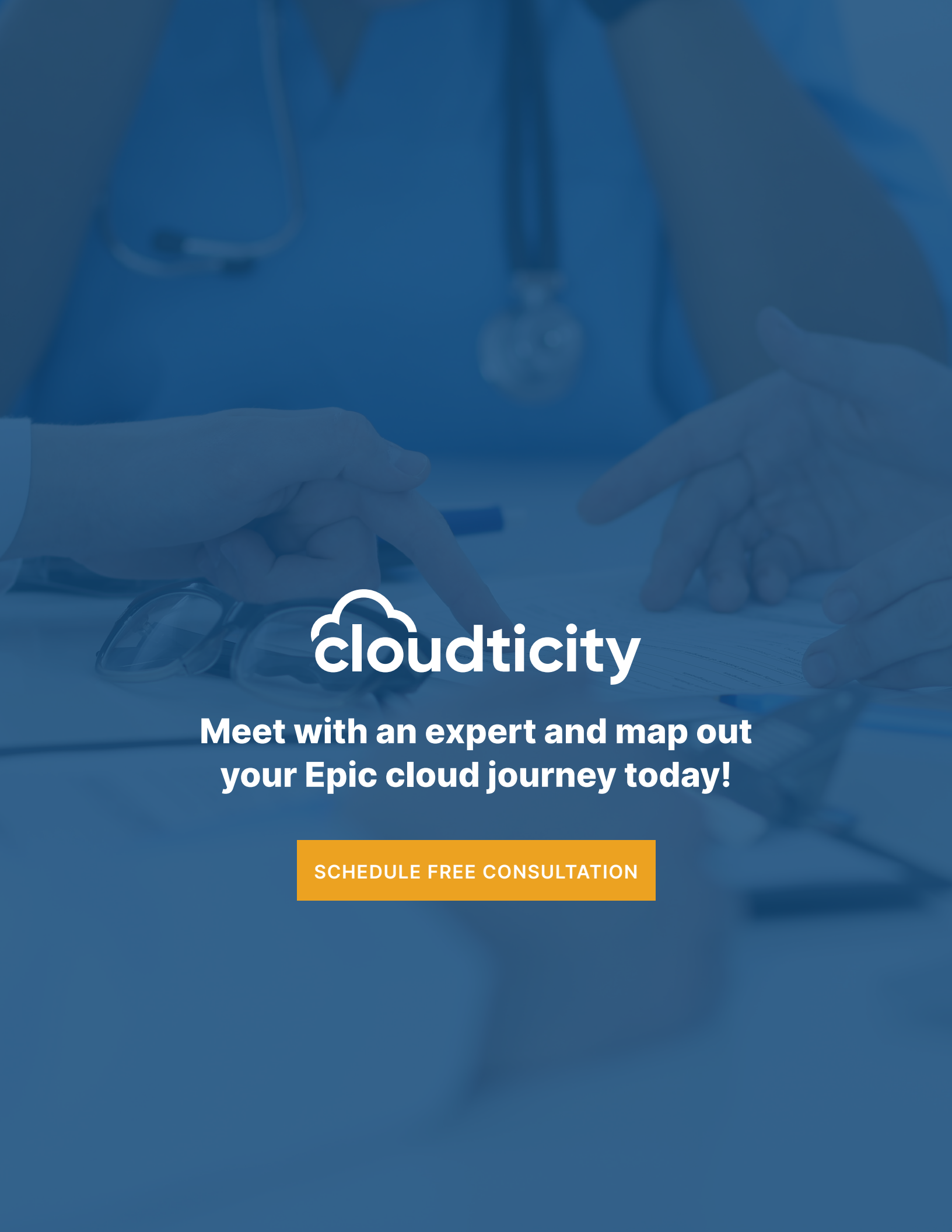
Distinguished for having built some of the earliest and largest health systems on the cloud, including:

- The first patient portal
- The first health information exchange (HIE)
- The first and only FISMA high deployment on AWS GovCloud
- The first Meaningful Use 2 (MU2) compliance attestation for a large hospital system
- The first COVID-19 registry for a state health department

Learn more at cloudticity.com.

ABOUT SAPPHIRE HEALTH CONSULTING

Sapphire Health was founded to solve a problem - CEO Austin Park (then an interim CTO at a healthcare organization) could not find a consulting partner with adequate expertise in Epic technical infrastructure. Sapphire Health now provides Epic infrastructure managed services to a variety of Epic customers across the United States and Canada. Sapphire also specializes in a range of services in the Epic infrastructure space including Epic systems BC/DR technical and process optimization, Epic infrastructure automation, and Epic platform migrations. With the experience of deploying, optimizing, and maintaining the Epic system, Sapphire Health is now leading the charge with Cloudticity and AWS to bring Epic customers into the cloud age.


cloudticity
Meet with an expert and map out your Epic cloud journey today!
SCHEDULE FREE CONSULTATION