Healthcare's Ultimate Guide to Cloud Migration

A ClearDATA Resource

CLEARDATA™

Cloud catalyst. Healthcare protector.

CLEARDATA™

Six Resources for Various Stages of the Cloud Journey

It's no secret that healthcare is experiencing a huge influx of technology and accelerating its digital transformation. Most healthcare providers are either in early stages of moving to the cloud or are preparing to move to the cloud this year. In fact, it is expected for healthcare cloud market to grow to $40.5 billion by 2025, which is an increase of more than $22 billion. Moving to the cloud can seem like a daunting task and is often the biggest challenge of digital transformation. But it doesn't have to be.

ClearDATA is here to help you along each step in your cloud journey.

Why Migrate to the Cloud?

Although there is no denying that migrating to the cloud is a big change, it's one accompanied by big opportunities. Here are the most significant reasons to move to the cloud.

1. **Cost-savings:** Cloud computing can be more cost-effective than traditional on-premises IT infrastructure because it eliminates the need for upfront capital expenses and ongoing maintenance costs. Plus, moving to the cloud helps reduce IT staff requirements and associated expenses.

2. **Scalability:** You can more easily scale up or down your organization's IT resources as needed to support changing business needs. For example, during a period of high demand, your organization can quickly provision additional computing resources to support increased traffic on your applications.

3. **Agility:** In the cloud, you have the agility to quickly respond to new business opportunities and market demands. If your organization needs to quickly launch a new application or service, your cloud solution will help you rapidly provision the necessary infrastructure and deploy the app, keeping you competitive and responsive to changing market conditions.

4. **Accessibility:** Cloud computing enables healthcare organizations to access data and applications from anywhere, at any time, on any device. This can be particularly beneficial for healthcare organizations with distributed workforces or patients who need access to medical records and other health information. With cloud services, you can provide secure access to applications and data from remote locations, allowing clinicians and patients to access information on the go.

5. **Compliance:** Cloud service providers can help healthcare organizations comply with industry-specific regulations and standards, such as HIPAA-compliant hosting environments, data encryption, and other security measures that are specifically designed to help healthcare organizations meet regulatory requirements. Additionally, you can access compliance reporting and auditing tools.

6. **Disaster recovery planning:** Healthcare organizations can finally work out their official disaster recovery (DR) plans. Switching to a cloud environment means organizations can create the DR plan necessary in an era of chaotic events, whether "acts of nature" or intentional acts of harm.

7. **Shedding the bloat:** This applies to costly service level agreements organizations no longer need after migrating to the cloud and that healthcare organizations are bound to uncover during an inventory check; equipment that's long been taking up space and even equipment currently in use but that will also no longer be needed in a virtual cloud.

8. **Cybersecurity:** Data breach attacks are only intensifying, now with state-sponsored hackers behind many of the attacks. A cloud solution offers advanced encryption, intrusion detection and prevention, and other security measures that are difficult or expensive for healthcare organizations to implement on their own. Additionally, cloud providers may have more advanced security monitoring and response capabilities, allowing them to quickly detect and respond to security threats.

Should healthcare IT departments really be expected to fend criminals off? Even if they could, they would have to devote all of their time to doing so. And IT professionals are needed for core business work, from health data analytics to preparing for major initiatives. At the same time, offloading IT management and security can go a long way in keeping an organization's reputation for protecting privacy intact. Too many others that are attempting to manage security in-house aren't having much luck with this.

Nor should they have to. A cloud solution (and top-tier service provider, if you go the third-party route) can these and other draining IT tasks for good. With all the advantages waiting to be tapped, it's no wonder that migrating to the cloud is a move so many healthcare organizations are making.

CLEARDATA™

Are You Still Trying to Budget Spend for Cloud Migration?

If so, the guide below, is for you. Shifting IT infrastructure costs over to the cloud and treating them as operating expenses (OpEx) offers significant financial benefits. Read this guide and get your CFO on board with the budget needed to move to the cloud.

Financing the Cloud: Considerations for Switching CapEx for OpEx

Although high-tech capital expenditures (CapEx) have traditionally been a source of pride and innovation among healthcare organizations, the storage requirements of today's data-rich environments are making those investments harder and harder to manage. The question is no longer if a healthcare organization will run out of storage and processing capacity; it's when. Add in a list of growing regulatory and compliance requirements, and the number of resources required to fully safeguard an IT infrastructure from outages, breaches, and non-compliance is massive.

Enter the public cloud. As a growing number of healthcare organizations are finding, shifting IT infrastructure costs over to the cloud and treating them as operating expenses (OpEx) can offer significant benefits. In fact, cloud migration is one of the top critical areas of investment for IT. This trend will likely pick up speed as the growth of the cloud services industry continues to skyrocket. A report from Global Market Insight projects that the global healthcare cloud computing market will achieve a 15% compound annual growth rate, exceeding $55 billion by 2025.

Of course, that's not to say that a major overhaul of IT expenditures should be taken lightly. Like any strategic decision, switching CapEx for OpEx requires business leaders to look closely at the short-term and long-term needs of their healthcare organization and weigh their options. This guide aims to help healthcare executives understand all the implications of financing IT in the cloud as an operating expense—the options, the benefits, and trade-offs.

OpEx Options

Selecting CapEx or OpEx is not always an either/or situation. Healthcare organizations simply need to assess their goals and decide which areas they want to bucket under CapEx and which areas they want to bucket under OpEx. The following are a few ways companies can divide up their IT spending.

1. Conservative Model

In recent years, most healthcare organizations have allocated for some OpEx within their IT budgets. The most common method has been to bucket all their hardware and equipment under CapEx, and bucket maintenance agreements and software licensing under OpEx. In some cases, an organization might end up putting maintenance agreements under CapEx since it extends the lifetime and usefulness of the equipment.

Many healthcare organizations currently use this model with success. In fact, it is not uncommon to find EMRs running on Parallel Random-Access Machines (PRAM) inside of a hospital or healthcare facility. However, this machine-based technology, which allows multiple processors to share memory, was introduced in the late 1970s. Organizations that have long-term goals to innovate, optimize their IT spending, and want to stay ahead of rising security threats and compliance requirements, may want to consider a more competitive model.

2. Infrastructure as a Service

Although many healthcare organizations are familiar with software as a service (SaaS), the next step is to shift their infrastructure to a service-based model (IaaS). IaaS allows an organization to run virtual machines or compute inside of the public cloud as an OpEx. This eliminates large capital outlays for equipment and puts the maintenance and upgrade responsibilities on the public cloud service provider or associated managed service partner.

3. Containerization

Another OpEx option is to containerize IT costs, so companies only pay for what they use when they use it. For example, a healthcare provider whose office is closed on the weekends could spin down all its excess IT resources or capacity during off hours and then spin them back up at peak periods. So, instead of paying to run their assets in a 24/7 environment, organizations "pay as they go." While this takes coordination through schedule tasks and automation, this can reduce operating costs dramatically over time.

4. Server-Less or Everything as a Service Model

Some leading-edge healthcare organizations have taken the full leap to OpEx and adopted a server-less or Everything as a Service (XaaS) model. A Deloitte survey reported that organizations are spending $20 million on XaaS and the majority plan to increase spend next year. XaaS not only frees up capital and other IT resources, but it also gives healthcare organizations the ability to pay only for the code they are running at times when a query was made. For example, when a provider or payer pulls a patient record, they might only have to pay a fraction of a cent inside of that public cloud to pull that query. Considerations here on the cost side include security tooling to monitor vulnerabilities within the code itself, as there is no longer infrastructure to scan, but instead code.

5. Hybrid Models

Although it is less common, there are some large healthcare organizations using both CapEx and OpEx strategically now to achieve their long-term goals of moving to OpEx. In these cases, the organization is running its primary data centers and primary facilities in a CapEx model, but bucketing its disaster recovery or burstability at peak periods into an OpEx model inside of the public cloud. The goal, however, is to move all of its PHI to the public cloud over time. By making a gradual shift, the organization doesn't have to buy new capital gear once that CapEx or those assets are fully depreciated, and it doesn't have to continue to build out data center capacity as more data is acquired. Cost savings is realized as OpEX driven maintenance on the software that is powering the data center equipment is not renewed.

OpEx Benefits

Once business leaders know their options, they need to weigh the benefits and possibilities. Although each company has its own reasons for making the switch to OpEx, the following are the main benefits it can offer healthcare organizations.

1. Financial Savings

Perhaps the most significant reason healthcare companies are moving to OpEx is the cost savings. As technology continues to advance at lightning speeds and the demands on IT infrastructures rise, it is getting harder and harder for healthcare organizations to keep their hardware and software up to date. Most companies outrun their 3- to 5-year capitalizations, and even if a company can stay within its projections and get a full return on their CapEx investments, refreshing those assets requires a huge capital outlay.

With an OpEx model, however, healthcare organizations have ongoing access to current technologies, unlimited storage, and the ability to scale easily according to their business needs. Instead of shelling out large upfront costs for equipment that is only going to depreciate, companies essentially "rent" their IT infrastructure for a consolidated OpEx cost. This monthly, "pay as you use" model is not only easier to budget when tools to measure public cloud cost optimization are in place, it also allows healthcare organizations to avoid overspending and frees up resources typically used to maintain CapEx investments. Also, because upgrading and maintaining the infrastructure falls on the service provider, healthcare companies avoid unforeseen costs like server downtime or network constraints and, instead, can spend their resources on core competencies.

2. Robust Security

Because healthcare organizations deal with extremely sensitive data, they can benefit especially from the enhanced security benefits that can come with an OpEx model. In CapEx, IT staff members spend an enormous amount of time and resources constantly patching their environments to protect them from cybersecurity vulnerabilities like malware, ransomware, and zero-day exploits. This doesn't just include patching the operating system inside of a hospital, for example, but also includes patching the hardware within the data center itself. And even then, there is no guarantee that the infrastructure is secure. According to one PwC study, 95% of provider executives think their practice is secure against cybersecurity threats; however, just 36% of providers and payers have access management policies in place, and only 34% have a cybersecurity audit process in place.

In an OpEx model, however, service providers with extensive security knowledge can be responsible for updating, protecting, and backing up the infrastructure. This layer of protection not only reduces risk for healthcare organizations, but it also frees up IT personnel to focus on other tasks.

3. Enhanced Compliance

Healthcare companies can also use OpEx to both guarantee and even exceed compliance. With standards like the EU's [General Data Protection Regulation (GDPR)]() and now U.S. state regulations changing and evolving, an OpEx model can make it easier for healthcare organizations to remain compliant. For example, GDPR's [right to be forgotten]() requires healthcare organizations to have a programmatic way to delete a patient record upon request. In a traditional CapEx model, this can be an extremely cumbersome and time-consuming as IT tries to locate every trace of a patient's PHI and then delete each of those traces. In an OpEx model, however, organizations would have access to native public cloud technologies that allow users to search for specific types of data through the use of tagging, as well as native public cloud machine learning tooling, whether it is PHI or non-PHI, so that they can be extracted and removed from the database architecture.

Many healthcare organizations are easing their compliance load further by working with specialized service providers that offer tools and services that guarantee compliance. Having access to this type of expertise — and the assurance that data meets HIPAA, GDPR, and other regulatory requirements — can relieve an enormous burden from healthcare organizations by fully protecting its assets.

4. Business Continuity and Disaster Recovery

Another huge benefit for healthcare organizations is reliability. By moving from a CapEx to OpEx model, business leaders are de-risking themselves over time because they can use newer technologies like the public cloud to build out disaster recovery plans without having to outlay additional cash for CapEx. This allows healthcare companies to be more efficient in their spending and use of technology resources, and it can speed up recovery time if an outage or disaster occurs. Instead of frantically trying to get systems back up and running and determining how much data may have been lost in an EHR system, healthcare organizations can work with a service provider to handle the situation and resume routine business operations with little to no downtime. Many organizations that are taking advantage of this model are building redundancy across public cloud geographies at the architecture level, to meet both business objectives but insulate themselves from any larger outage event, while keeping their cost down by using the second geography as a standby (or warm) site.

5. Ability to Innovate and Grow

Although healthcare is known for its vertical integration and medical advancements, it has traditionally struggled with horizontal innovation. OpEx drastically improves the ability for healthcare organizations to embrace new technology without the risk or large upfront costs. Providers, payers, and other healthcare organizations are no longer stuck in 3- or 5-year agreements with the same capital gear inside of their facilities. With OpEx, healthcare organizations can upgrade as needed and look at more transformative innovations. So, for example, if a provider wanted to experiment with permissioned blockchain technology to help secure PHI, an OpEx model would provide that opportunity.

The flexibility of the OpEx model also enables healthcare organizations to be more agile. Companies have the flexibility to scale instantly both horizontally and vertically without having to invest in expensive equipment or services.

6. Improved Speed to Market

The speed to market is significantly greater in an OpEx model. Let's say, for example, a healthcare provider is looking to deploy new facilities. Using a traditional CapEx model, it could take anywhere from six to nine months to go through the entire process of getting the IT infrastructure in place: negotiating the capital spend; picking the vendors that align with the security requirements for healthcare data; ordering the gear; negotiating a business associate agreement with each hardware vendor that may store, process, or transmit PHI; setting up power and network in the data center; and finally, installing and provisioning the gear and providing access to the right people. However, if the provider decided to use an OpEx model, it would eliminate all of the equipment and set-up, cutting the whole process down to mere weeks.

Faster time to market can play out in everyday use cases as well. In a public cloud OpEx model, for example, a healthcare organization can save time by using reference architectures or blueprints that other organizations have successfully used to deploy a secure and compliant infrastructure. Depending on the application, this could cut deployment down to minutes, hours, or in a worst-case scenario, a few days.

OpEx Tradeoffs

Of course, a number of business leaders have reservations about moving to a cloud based OpEx model. While there are always some trade-offs when taking a new approach, the key is weighing business needs and goals against risks. The following are a few of the common arguments against switching CapEx for OpEx.

1. Lack of Control

Many healthcare organizations prefer having full control over their data and equipment. Plenty of IT leaders have spent a lot of time and money building a protected, secure infrastructure. The problem is that in today's market, it is extremely hard for companies outside of the tech space to keep up with the pace of innovation, rising security threats, and evolving compliance requirements. The reality is that CapEx equipment in any environment now runs the risk of being outdated and vulnerable on a daily basis.

Put simply: It would be extremely rare to find a healthcare provider or payer that could build security tooling inside of its own data center faster or better than Amazon, Microsoft, or Google cloud services. In the end, healthcare organizations that move to an OpEx model with experienced service providers will actually have more control over their infrastructure because they will have the assurance it is updated, secure, and compliant.

2. Inability to Capitalize Hardware

As any executive understands, the whole reason for positioning items as CapEx is the return on investment. CapEx provides predictable tax deductions and usually benefits gross margins. OpEx expenses, on the other hand, don't necessarily pay for themselves and are often known for causing business debt.

In general, these arguments are accurate; however, when it comes to aging IT equipment and unpredictable storage needs, CapEx falls short. OpEx not only provides more value from a scalability point of view, but it can also benefit the bottom line. OpEx items can be fully tax deductible and can be subtracted from revenue when calculating profits and loss, all of which generally increases profit margin. So while a move to OpEx will impact gross margin and change the financial economic model, it isn't necessarily a negative change. Costs are just falling below the capital line and hitting a different bucket on the financial balance sheet.

3. Cost Containment

Another key argument against OpEx is cost containment. This is a valid concern. In cloud based OpEx models, users are essentially given the ability to log into a virtual portal or virtual appliance and spin up unlimited assets, unlimited servers, and unlimited resources. This can be hard to control and can quickly become a real issue for IT budgets. As a result, healthcare organizations need to be diligent and put tools and controls in place to help manage IT spending. This includes implementing internal controls like training and policies, as well as external controls like Cloud Checker, Cloud Health, or other software tools that can provide alerts when a budget is maxed out or exceeded.

Financing the Future

Looking at a new financial model for IT spending is a big decision — one that should be more about business needs and goals and less about bandwagons and buzzwords. However, a growing number of healthcare organizations are finding that with the right partners and expert resources in place, switching IT spending from CapEx to OpEx can enhance security, drive innovation, and improve the bottom line. By understanding the benefits and trade-offs of OpEx, business leaders can find a solution that meets the current needs of their organizations while also positioning their business for future success.

Is Staffing a Roadblock to Move to the Cloud?

Everyone knows that there is a major shortage of cybersecurity and cloud expert resources, especially in healthcare. Some providers put off moving to the cloud thinking that they don't have the resources to do it. However, you can augment your existing team and save time by moving to the cloud. This allows your team to focus on other business goals and have more time to bring innovative technologies that solve healthcare problems. Read the guide below for more information.

How to Augment Your Existing Team to Remain Focused on Core Competencies in Healthcare

Today's healthcare IT leaders and their teams have more responsibilities than ever before. Whether struggling to keep assets up to date, dodging nonstop security threats, or dealing with the tsunami of data that continues to spill into their systems, teams have little time to focus on core competencies like innovation and improving patient care. A conversation with Chris Bowen, Chief Information Security Officer and Founder at ClearDATA, reveals there is a way for IT teams to stay mission-focused without compromising security, privacy, and compliance. Bowen discusses: the challenges today's organizations face, when healthcare leaders should consider leveraging external resources, and practical strategies for getting teams back on track.

Q: What might happen within a healthcare organization to make them start thinking about augmenting their team?

Bowen: There are several reasons to think about augmenting a team. It could be a business case that compels you to do something more innovative. It could be a merger or acquisition. Maybe an organization needs to consolidate from a physical data center and move to the cloud to save costs. Maybe it is because a leader in the organization has moved to another organization and taken with him or her some of the internal expertise. Maybe it is a combination of all that. Maybe it's just a doctor asking, "Why can't you do this faster?"

Q: What are some of the day-to-day activities that can inhibit an IT team from focusing on core competencies like innovation, maintaining a competitive edge, and improving the patient experience?

Bowen: As an IT team member, If I don't spend my time hardening operating systems every time they come out with an update from CIS...If I don't have to manage my security groups in a way that can be manually intensive...If I don't have to patch every Tuesday that Microsoft comes out with an issue to fix... If I don't have to do all that — if that can happen for me — then it allows me to spend my time doing other things like enhancing my data model, making sure that I can service the requirements that my own customers have of me. If I don't have to spend my time 'blocking and tackling,' doing some of the basics around privacy, security, and compliance within my infrastructure and my services that support that, then I can work on my application and enhance that and make it better.

It comes back to servicing the patients, fulfilling the mission, and allowing me to bring to market innovative technologies that solve healthcare problems.

Q: What are some signs that it's time to refocus your internal resources back to your core competencies?

Bowen: Typically, it's around the skills of the internal team. If I am a payer that wants to better engage my members, I need to do something radical and bold — maybe it's using a new service. To enable that, looking internally can be a challenge because you've had resources aligned with traditional data initiatives or with traditional infrastructure, technology, or security initiatives. (This happens in every kind of organization in healthcare by the way, not only payers.) We've seen the biggest of the big go through this, and what they've learned is there needs to be some sort of infusion of expertise to succeed. Companies are typically able to invest in those resources — bringing in third-party experts — and of course they want to make sure they utilize their people where they can, but it's frequently the case that they just don't have the expertise to be able to achieve what they need to in a way that gets them to market fast enough.

Q: Do you think this is more of a challenge today than it has been in the past?

Bowen: I think so. The number of breaches on record for healthcare continues to increase year-over-year, as well as the digital transformation and increase of data liquidity expand the attack surface. If you think about it from the perspective of a healthcare organization, there's a lot to learn. They have to figure out: "How do I use artificial intelligence? How do I leverage machine learning? How do I leverage containers and serverless technologies? How do I make sure my storage is locked down and that logs are flowing properly? How do I bring all these tools together in a way that gives me a smaller risk profile?" Many times, an IT team does not don't know how to do all that, plus service patients, members, and bring that new device to market. If my focus should be on solving healthcare problems, why would I as an organization spend my time trying to figure out how to manage vulnerabilities when I can use the automation of a partner to manage that for me?'

Q: Do you think the cloud is part of the solution?

Bowen: Absolutely. But the cloud journey is a shared one. There are certain things that a customer must do and a lot of things that the cloud provider must do. Many times, the shared journey gives the customer the ability to outsource or leverage the cloud provider and offload some responsibilities. What we have seen is that certain segments within healthcare have done a lot more adopting of cloud compliance automation and risk remediation automation. There are many within healthcare that are really good at cloud, and then there are those that are just now starting to dip their toes into the cloud and really need some help in how to get there.

Q: Why is it a good idea to consider leveraging the skills of a third-party partner like a cloud services provider?

Bowen: Thinking as a business or IT leader in any healthcare organization, I would go back to looking at the knowledge and bandwidth of my team. Does my team have the time to dedicate to learning every HIPAA-eligible cloud service, creating the reference architecture, updating the tooling around service updates, etc., versus what the business imperatives are that our organization must accomplish?

As a business leader, my job is to help my organization accomplish our mission. In healthcare, typically that mission is to solve or address a significant healthcare challenge. If I can leverage a third-party company or a provider that already does a lot of the blocking and tackling for me that I mentioned previously, then I can focus on my core mission and core competencies. It's truly that simple. Once I'm freed up to focus on the mission, I can use my scarce resources to work toward solving the cancer problem, the Alzheimer's problem, or figuring out a way to keep patients on their rehabilitation plan, for example. I can find time to develop a program that transports a patient to a doctor's appointment using Lyft or Uber. I can figure out a way to help people eat healthier to help prevent chronic conditions and the costs associated with those conditions.

In that role as a business or IT leader at a payer, provider, healthcare IT, or life sciences organization, my job isn't to leverage and become an IT expert on cloud compliance and security; my job is to fulfill the mission of my organization. As a leader, the way I can best do that is by using my resources in the most effective way.

Q: Would you say enhanced security is a benefit?

Bowen: Absolutely! I would bucket that into the blocking and tackling referenced earlier that can eat through any healthcare organization's time, resources, and personnel. What are the table stakes? How do I protect my data? How do I know where the data is? How do I prevent my data from suddenly being copied over to a region in France when it's not supposed to be outside of Hong Kong, for example? You can now move data across the globe with a couple of clicks. How do you stay safe? When you're asking these questions all day long, you aren't left with the time to innovate and address the healthcare challenges in front of you.

Q: Are there any financial benefits to augmenting your team?

Bowen: Yes, there definitely can be. For many of the organizations I work with, augmentation of their team has translated to faster time to market. If I have innovation that I need to deploy to capture market share or to attract more patients, then I'm going to leverage somebody who can get me there faster. If I want to be more agile and go faster, then I'll do that. If I want to do it in a more secure manner or if I want to offload some risk, I'll use a partner. If I want to leverage an OpEx model versus a CapEx model, then I'll do that as well; maybe that helps my accounting and my budget scenario.

Q: For a strategic business leader looking to scale, what are some of the third-party services to consider?

Bowen: I would certainly say the management of your network, backups, and resilience can all be offloaded to cloud services; managing your redundancy can be automated. You can use microservices and tracing tools to trace your data throughout its journey within a Kubernetes environment, for example. You can better track your data flows and your data sprawl — all in effort to remove yourself from some of the blocking and tackling and really going out there and building a strategy to make your patients' and members' lives better. And let's not forget that HIPAA Security Rule requirement around system activity reviews. Leveraging a third party to watch your logs for any anomalies 24/7/365 is a huge resource drain. Why not leverage a third party designed to do just that?

Q: Would you say there are any drawbacks to working with a third-party partner?

Bowen: I think it depends on the partner. Like so many things in life, it's about due diligence. If you have someone who is focused on some proprietary way to do things instead of abstracting and using multi-cloud approaches, you may want to reevaluate that. There are a lot of things to consider. How many incidents has the potential partner been responsible for reporting as a breach? What is their maturity level from a security and privacy perspective? How do they demonstrate that? With which organizations does the partner do business? Who are their investors? Will the partner be around for the long journey ahead? Are they HITRUST certified? That last question is a great starting question in any search for a third-party partner.

Q: How can a healthcare organization work with a third-party partner like a cloud service provider and still maintain their existing IT team?

Bowen: I'm glad you asked that question because sometimes a company will say to me, "I don't want my people to be let go." What I tell them is bringing in the right third party can enhance your team's skills. Instead of having your employees focus on basic things like patching and systems hardening, teach them a new trade, teach them how to leverage the cloud for their own purposes in the organization. Teach them about micro services, teach them about containers, teach them to be innovative within their organization. Then actually let them innovate instead of focusing them on commoditized tasks that can be done with certain automation. I would also say to use a partner that can help them learn and grow while it builds and protects your business. Also, most healthcare organizations, especially in security, are understaffed and lack the necessary resources.

Q: Any final words to healthcare organizations considering third-party support for cloud compliance or other cloud services?

Bowen: I like to think about it in terms of leveraging…it's like borrowing muscle rather than lifting heavy things yourself. As a business leader, I am going to leverage the expertise of the cloud, and I am going to leverage the expertise of the billions of dollars that the cloud providers have invested in security automation, for example. I'm going to leverage the expertise of those who have built cloud systems in healthcare for years and years and years, who now are our high-level partners with the major cloud companies that have expertise in healthcare. I am going to leverage all of that, absolutely, if I'm a company that really wants to jump into the cloud in a way that propels me to the fulfillment of my mission.

Are You Debating on Building Versus Buying?

Taking a DIY approach will require a lot of internal resources, technical talent, and healthcare compliance and security expertise. The guide below summarizes the three stages of DIY cloud and lists all the things you need to consider if you think building is the way to go.

Build Versus Buy: Finding Your Payoff in the Healthcare Cloud with the ClearDATA Platform

As a leader in healthcare, you know some business objectives are more complex than they look on the company strategic plan. Take a directive like "Migrate to Cloud" for example. It's not as simple as just determining which workloads you want to move, doing a lift and shift, and paying your cloud provider for your resources. Like purchasing a car, there's more at stake than picking a model and grabbing the keys. There are other considerations like safety features, mileage, capacity, tax, title, license, insurance, security and anti-theft, and ongoing maintenance. The cloud is similarly not a singular decision.

The DIY or DIWH (do it with help) decision can turn into a lengthy debate. In the end, there are two things it pays to focus on: time and talent. How much time do you have to get it done and do you have the talent in-house to maintain adequate security and compliance?

You're going to need very specific skill sets that simply didn't exist a few years ago and that is a challenge to find in the workforce. At ClearDATA, we partner with hundreds of healthcare organizations both large and small – from providers to payers, healthcare IT to life sciences, and pharma. Many of them do not have the cloud-certified solution architects and product and software engineers that you'll need to get the job done right.

At ClearDATA, we spend a lot of time and money hiring and training staff focused on cloud, cybersecurity, and compliance specifically for healthcare. It's expertise that helps healthcare organizations like yours reduce capital expenditures and pay only for the cloud resources you need on a consumption basis, making it a more cost-effective option. Our staff also builds a solution that allows for quick and easy scaling up or down, depending on the organization's needs, without the need for significant infrastructure investments. By partnering with a cloud service provider, you can leverage extensive expertise and infrastructure to reduce your risk and ensure that your cloud solution meets all regulatory requirements.

Building and managing a healthcare cloud solution can be a time-consuming and resource-intensive process, taking time and resources away from core competencies such as patient care and research. By partnering with a cloud service provider, as a healthcare organization, you can focus on delivering your core competencies while leveraging the expertise of the cloud provider for your technology needs.

That talent is in high demand as healthcare, like all other industries, moves to the cloud.

So, you may be wondering, or more realistically, your CEO or COO may be asking, "Is it more cost effective to do this ourselves or to go with ClearDATA?" Let's look at the three stages of building and deploying your app in the cloud to help you identify the cost of sourcing internally. Then, you can contact us, and we'll show you what it looks like to have us be your cloud partner, freeing you up to focus on your business objectives.

Phase I: Getting Started

Business Associate Agreement

First and foremost, you'll need a Business Associate Agreement with your cloud provider. While ClearDATA will negotiate a purposeful BAA designed to meet your specific and unique legal and business needs, cloud providers seldomly are able to negotiate the BAA with you. So, plan to allocate what can turn into several hours with your legal department trying to get these taken care of. In addition to a BAA signed with the public cloud, you will need to manage a BAA with other subcontractors or other third-party vendors.

Operations

It begs the obvious, but to get started one of the first things you'll need is a team. This may mean recruitment and staffing in addition to training and alignment. You'll also need a security risk assessment as a starting point and, if you haven't already done one, a PHI inventory. If you haven't already made the decision on which public cloud you want to use – or more than one – you'll have to vet your options. Pricing and services vary. ClearDATA has deep relationships with all three clouds: AWS, Google Cloud Platform and Microsoft Azure including premier consulting partner relationships where applicable. We understand what they offer and can help design your cloud architecture to leverage the most appropriate and effective services based upon the needs of your application.

Cloud

Now it's time to build your cloud infrastructure (or, ClearDATA could). This will include:

- Integrating hardening standards into your infrastructure as code pipeline.
- Developing infrastructure and service hardening standards.
- Building infrastructure as code deployment pipeline.
- Automating dependencies for chargeback into account and workload management.
- Internal chargeback and budget management strategy.
- Implementing account management automation.
- Developing account segmentation strategy.
- Implementing access control system.
- Developing access control governance strategy.

Phase II: Compliance and Security

This is where it gets a lot more complicated. We talk to many healthcare organizations that become our customers at this phase because although they were able to build and deploy within compliance frameworks, data is not static, and they drifted out of compliance the moment anything changed, and more importantly risking the integrity of data security. They also realized the cost and risk associated with not having the deep expertise in healthcare's regulatory environment and the time and resources needed to commit to managing and monitoring security and compliance in the cloud. The reality is to be really good at the business of privacy, security and compliance in healthcare, it needs to be your only business because it takes extensive time and resources.

You'll need to dedicate some serious time to reading and interpreting some of the newer regulations like the General Data Protection Regulation (GDPR) and state specific regulations, or HIPAA that was written some 20 years before any of the technology we are using today actually existed. And it's important to remember and remind your team: just because a cloud provider offers HIPAA eligible services doesn't mean they've taken care of your compliance stature. It's up to you to not only configure your HIPAA eligible services in a manner that makes them HIPAA compliant, but also ongoing compliance throughout the use of the service, and for a lot of organizations that's a huge gotcha that leaves gaps that increase security risks. And we know risk equals time and money with a layer of worry on top. Read this article to learn more about the difference between HIPAA eligible and HIPAA compliant cloud services, Here's what you'll need to be ready to address for your compliance and security posture in the cloud:

Compliance

- Compliance experts who regularly review and interpret complex healthcare regulation standards, both new and old, including:
- HIPAA technical safeguards to protect electronic protected health information (ePHI), as well as regular risk assessments and workforce training.
- HITRUST certification to demonstrate their compliance with multiple regulatory frameworks, including HIPAA.
- General Data Protection Regulation (GDPR) compliance, which regulates the processing and protection of personal data.
- Ability to map and align technical controls across regulatory frameworks and standards.
- A strategy for monitoring your compliance and security posture and supporting ROE.

- A method of governance, enforcing compliance through adherence to documentation and/or code, including:
    - Establishment of policies, standards, and procedures for cloud usage, including data governance and management.
    - Monitoring and reporting on cloud usage, including user activity, system activity, and resource usage.
    - Clear roles and responsibilities for cloud management and oversight.
- Based on geographies of where you're working, identification of any data sovereignty requirements.
- A data locality plan.
- Determination of your auditable measurements for mapped technical controls.
- Visibility into ongoing compliance stature via a dashboard, or some way to show your compliance in an auditable trail.
- Audit strategy for delivering ROE detailing compliance.
- Annual audit support.
- A compliant container and microservices offering including Kubernetes.

Security

- Hardened images according to CIS benchmarks for numerous operating systems, patching every night, with releases every 30 days.
- Intrusion detection for monitoring, along with a team of experts to detect and prevent any malicious attacks.
- A security incident management plan that addresses the ability to identify, protect, detect, respond, and recover from a security incident.
- Vulnerability scanning and remediation.
- A system for monitoring product assets.
- Defined strategies to enforce key management, log retention, data protection, encryption, and more.
- Implementation of appropriate access controls and user authentication methods.
- Use of encryption to protect data in transit and at rest.

Resilience

- Development of a comprehensive disaster recovery plan that includes backup and restoration procedures, and business continuity planning.
- Implementation of a high availability architecture that minimizes downtime.

Phase III

Phase III is the ongoing day-to-day concerns about security and compliance as you work to scale your business and find time to focus on your business objectives.

We speak with many organizations that can do some, but not all of the work in these three phases. For them, we offer a la carte services and products in a self-serve model, so they only pay for what they need. For other organizations we talk to leaders who need it all, start to finish, so they can get on with building their business efficiently.

We increasingly see many that want ClearDATA to step in for the actions outlined in this document because they want to focus on being in the business of innovating healthcare outcomes, growing their business, and expanding their digital transformation efforts. If you put a pencil to what it would cost you to do this as a DIY adventure, we think you'd see time and money saved by going with a company that does this as its business every single day and whose mission is focused on finding new, safe ways you can innovate in the public cloud.

Learn more about how ClearDATA helps give you more time to focus on your business objectives with our CyberHealth™ Platform.

No One Is Perfect!

You're not alone — most providers stumble along the way when pursuing their digital transformation and cloud journey. Learn how to avoid frequent pitfalls we see from helping hundreds of healthcare organizations move to the cloud.

Common Mistakes Providers Make in Their Digital Transformation Efforts

Introduction

Whether they lack the deep technical expertise or try to make do with do-it-yourself efforts, healthcare providers often stumble when pursuing digital transformation efforts, such as moving patient data into the cloud or creating successful engagement with patient portals.

Frequent Pitfalls Providers Face in Digital Transformation

Digital transformation can improve your business agility and consumer experience. You can leverage cloud to store and utilize patient data securely, comply with federal and state healthcare regulations, improve patient care with data-driven treatments, and increase transparency of price and control costs. However, when improperly implemented, digital tools can hinder rather than help you. In fact, 96% of organizations have experienced significant challenges when implementing their cloud strategy. The top cloud challenge? Of all respondents, 85% of organizations said security.

So why is security such a challenge? The same research found that public cloud spend is over budget by an average of 13% across all organizations. According to Statista, the top cloud security concerns are data loss and leakage (69%), and data privacy/confidentiality (66%), followed by accidental exposure of credentials (44%).

Despite being aware of these challenges, only one in five organizations assess their overall cloud security posture in real-time.

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

- Rushing to adopt new technology without a thorough assessment and fully understanding their current state and future goals.
- Focusing on apps or solutions first, and then trying to rationalize security and compliance as an afterthought in the process.
- Not engaging key stakeholders throughout the project, including aligning with IT business goals.
- Migrating to the cloud without a plan for future growth and scalability, which can lead to unexpected costs and inefficiencies down the road.
- Trying to go through digital transformation alone instead of tapping the expertise of third-party vendors.
- Security risks posed by insider access. 32% of organizations have unnecessary privileged access for users that don't need it.

Digital transformation tools have the capacity to reshape how you provide patient care, while also helping you improve operational efficiency. But you'll want to be sure to avoid these three common pitfalls, because they will slow down digital transformation efforts and put you at risk for costly security and compliance issues.

Build With Compliance Front and Center

Data breaches in healthcare are more costly than in any industry, and the reputational damage organizations face is significant. A culture of compliance and security not only reduces the likelihood of a breach, but also lessens the cost in the event of a breach. Compliance and security must be front and center in every digital transformation effort. Too many organizations concentrate on building their app or solution first, and then try to fit compliance and security into the solution. With a compliance and security first culture, you will end up with a better, more secure solution. For organizations that don't know where to begin, work with third parties who have compliance and security baked into everything they do.

Engage Key Stakeholders

You need to engage stakeholders throughout the digital transformation process. Digital transformation efforts are less likely to succeed when they have blind spots and siloed information. For example, one reason why some electronic health record implementation efforts fail is because providers build digital tools for clinicians without obtaining clinician feedback. The sooner you engage your influencers inside your organization, the more successful you'll be. That's especially true for executive staff such as the CISO (Chief Information Security Officer), who is legally obligated to be sure any security risks are taken into account in your planning and implementation. It's critical that whenever you build and deploy new technology, you're building an engaging user experience, and that means including your stakeholders and end users in the process.

Leverage the Expertise of Others

While healthcare providers have a unique set of requirements and challenges, they can take advantage of the fact that they aren't the first healthcare organizations to undertake digital transformation projects. Providers can look to other healthcare segments like payers, and even non-healthcare early adopters, for insight into possible pitfalls and inspiring success stories. Additionally, leveraging the experience of third parties to support areas of digital transformation that are challenging for your organization can save money and improve project outcomes. A survey by Masergy found that 64% of enterprise IT professionals reported needing third-party support to meet their digital transformation goals. Because digital transformation projects in healthcare often involve changing the way protected health information (PHI) is managed, some providers seek third-party support in managing their cloud compliance efforts so they can remain focused on core business goals.

Where Should You Start?

To avoid many of these pitfalls, providers may want to start their digital transformation efforts with small pilot projects that are less costly and risky yet offer potentially large returns. For example, many begin with portals that allow patients to schedule appointments, request prescription refills, or manage preventative care. Others have started by moving data storage into the cloud as that technology has improved and become more secure. As technology advances, many organizations realized they need virtual care to remain competitive and have increased investment in virtual care technologies. Then the pandemic greatly accelerated the demand for virtual care.

Ultimately, start with the less risky aspects of digital transformation and then move to more sensitive items. After success with initial projects, you often will see exponential growth in the use of digital as comfort levels, trust, and experience increase.

Digital Transformation Can Pay Off

When done correctly, digital transformation can provide you with substantial benefits. It can increase price transparency and provide new ways for you to connect with consumers. It also can help improve quality of service because it will enable you to make more informed decisions for personalized care – something patients have learned to expect as industries like retail and banking have reached digital maturity.

Digital transformation can allow you to better engage patients, reduce cost, increase efficiencies, and improve quality of care. In addition, it can allow your organization to remain competitive in the evolving transformation of healthcare.

Digital transformation can increase your profitability. Research shows providers having shrinking revenue and increasing costs as the industry pivots away from fee-for-service models. And the digitally transformed organization using big data or machine learning experiences increased efficiencies and competitive edge over others in their market.

The New Digital World

Digital transformation is changing the way providers do business and is revolutionizing patient care in an era of shifting healthcare economics. As patient outcomes become a critical variable in the reimbursement equation, providers must be able to deliver personalized, data-driven treatments and ensure patients adhere to treatment plans and take their prescriptions.

Without digital transformation, providers face a bleak future as healthcare costs, especially for chronic diseases, continue to rise. The Centers for Disease Control states that that 90% of healthcare costs are spent on chronic diseases and mental health issues. Personalized care through digital transformation can help prevent chronic disease in many cases and better manage it in many others. The end result is healthier patients and lower costs.

Healthcare providers may face pitfalls when approaching digital transformation programs. Failing to navigate around these challenges effectively can make a difference not only in whether a provider can improve its own operations, but also in its ability to meet increasingly complex security and compliance regulations. On the flip side, successful digital transformation programs hold the potential to improve patient care and outcomes dramatically while generating substantial cost savings for providers.

Need Help Making Compliance & Security a Priority?

We all read daily headlines about healthcare experiencing another ransomware attack or reporting a data breach, and every now and then we read about the latest OCR settlement for non-compliance. Making security and compliance a priority is necessary when moving to the cloud. Read this article to learn how to overcome some of the top security and compliance challenges when moving to the cloud.

How to Overcome Security and Compliance Challenges When Moving to the Cloud

This content is adapted from a webinar of the same name.

Thanks to the passage of the HITECH Act more than a decade ago, the healthcare industry is well on its way through a major digital transformation. Yet, when it comes to embracing the cloud as a vital tool for enabling transformation, healthcare organizations tend to move slowly and cautiously. Nevertheless, seeing the tremendous benefits that other industry verticals reap from migrating to the cloud, healthcare is finally on board. Healthcare organizations are rapidly moving their clinical data and applications to the cloud.

If you're an IT leader in healthcare and moving to the cloud, there are several considerations to keep in mind from a security and compliance perspective. In this article, we'll look at some of the most pressing ones.

Assess Your Team's Cloud Security Knowledge

Before you can move to the cloud, it's important to figure out where your current security challenges lie. To do so, look at your talent from an outside-in perspective to understand whether they'll be able to grow and evolve with the business as you continue to innovate and migrate to the cloud. Specifically, you'll want to know if they're up to date on security tooling and all of the latest advances in public and private cloud. If they're not up to speed, investigate cloud security training programs from public cloud organizations and third parties. You'll also want to ensure that you have the right security tooling in place for them to use and that they understand how that tooling maps against your policies and procedures, as well as the various regulatory requirements in every governmental jurisdiction in which you need to adhere.

Make Sure You Understand Data Flows and the Need for PHI Inventories

As a provider, you need to understand your PHI inventory, including where your data lives, how it flows through your applications, and the safeguards in place to protect it. Of course, given that doctors, nurses, and other healthcare providers are constantly moving medical images, notes, patient records, and other forms of PHI from one application to another, that can be a real challenge. Not only that, but you also need to understand exactly how your data is secured as it relates to all of that PHI and how cloud-based telemetry and alerting works when potential issues arise.

Know the Advantages of Using Automation and the Impact if You Don't Automate

While most people talk about automation in terms of increasing their velocity, it's also important to look at its advantages from a security and compliance standpoint. In healthcare, automation can bring three valuable benefits from this perspective: 1) the predictability that every time you deploy something it's going to get the same results, 2) the ability to move quickly in terms of security remediation, and 3) a reduction in manual work and human error by enabling auto-remediation. Fail to take advantage of the automation that comes with moving to the cloud, and you could be exposing yourself to unnecessary risk.

Use Augmented Encryption for Protecting PHI

Encryption is a critical factor for securing PHI but it's not as simple as that. For starters, you must consider encryption from many different angles, including encryption at rest and encryption in transit. You also need the right security tooling to augment your encryption. Importantly, that tooling needs to leverage cloud-based key management technologies and be monitored and reviewed with a centralized system like a security information event management (SIEM) system that drives alerts, aggregates logs, and correlates events to help augment your vulnerability management and encryption strategy. Finally, you also need automated discovery of anomalous activity to generate alerts and drive action.

Mitigate Negative Impacts from Shadow IT on Your Organization

Shadow IT exists in most large organizations and is often unavoidable. The problem is that when you have systems that are undocumented, unmonitored, or unpatched, it can expose your organization to serious risks. Further complicating matters is the fact that with shadow IT, there's no PHI inventory mapping, and certainly no safeguard integration. Finally, consistency is a major consideration. With shadow IT, there's always the risk of inconsistent hardening and mapping of controls - if any -and regulatory adherence to regulations like HIPAA, GDPR, and any others you may be required to follow.

Utilize Security Risk Assessments to Find Security Gaps

Security Risk Assessments (SRAs) play an important role in detecting security gaps. During an SRA, it's important to identify where PHI may be, the safeguards in place to protect it, and a plan for remediating any gaps in protecting that data. That plan should include a security risk register that shows the steps you're taking to remediate and allows you to track your improvement. If you take the approach that you need to work to improve your compliance every single day, and that it's a journey rather than something you can achieve overnight, you'll be in a much better position to succeed. Make no mistake, however, in a reportable incident, one of the first requests from the Office for Civil Rights will be documentation of your risk assessment.

Know That Not All Clouds Are Created Equal

When selecting a cloud vendor, due diligence is critical to ensure that you're making the right choice for your business. To do so, make sure you think about what problem it is that you're trying to solve. Technologists tend to get caught up in a lot of details like price and functionality, without ensuring the vendor can actually solve the problem at hand. Other things to consider include mapping the public cloud vendors' capabilities back to your use case and recognizing that not every cloud provider offers HIPAA eligibility for all of their associated services. (By the way, even though the cloud may offer HIPAA eligible services, it's up to you to configure and deploy them in a way that's HIPAA compliant every day going forward). Finally, understand where liability sits with each of your cloud vendors, as well as your security and compliance vendors so you know what to expect.

Moving to the Cloud

If you're thinking about moving to the cloud, you know there's a lot to think about. Security and compliance should always play an important role in shaping your decisions. By keeping the considerations outlined above in mind, you'll be in a much better place to ensure that your migration to the cloud is smooth and successful. Better yet, partner with a vendor who has done it thousands of times and can navigate these issues for you.

CLEARDATA™

Have You Decided You Need a Third-Party Partner?

If so, smart choice. There are a lot of benefits to finding the right partner that can function as an extension of your team to help you migrate and manage your cloud services. To do so, we find that many healthcare organizations need an RFP, so we've put together this guide to help you.

Guide to RFP for a Cloud Services Partner Focused on Security, Privacy & Compliance

So, you've decided you want to take advantage of the public cloud to transform and grow your organization's digital transformation. That's a smart move. You've likely also decided you want a third-party partner to support your privacy, security, and compliance needs, because you work in healthcare and those considerations are table stakes. You may not need an RFP, but many people do, especially if you are bringing public cloud to your healthcare organization for the first time. There are several key considerations to bear in mind when opening your cloud services RFP. This guide will help you through the process and provides some important questions you'll want to include in your RFP.

The first and most important thing to bear in mind is that healthcare is a highly regulated industry, and the cloud is a constantly evolving platform, so there is a convergence of enormously important security and compliance concerns alongside expanding opportunities to use cloud native services to transform and innovate. You can use the cloud to optimize costs, scale with agility, and provide better protection for your organization than you can in an on-premise environment, but you'll want healthcare-exclusive expertise because of the complex nature of healthcare regulatory frameworks. If you're already in the cloud, you're probably seeing some great opportunities, but may be losing sleep over concerns about the security of your PHI. Help is out there.

The first piece of advice I want to offer as you prepare to write your RFP is to be specific, but don't box yourself or your RFP respondents out of opportunities you may not have considered. Focus on the desired business objectives and outcomes you want to attain. Focus on performance, ask about both deliverables and how success of those deliverables are measured, and check references for expertise. Think about the details and be deliberate but try not to be overly prescriptive in how you frame your questions about how respondents can help you meet your business goals. By focusing on the objectives, you'll allow the respondents to bring forward solutions to your business challenges that you may not have considered. They will often share a new perspective that may evolve your design, execution, or even selection process of the RFP itself.

That said, you want a well-designed, thorough RFP and your procurement process must include due diligence. Not all cloud platforms are created equal. Get details. Do your homework.

Timelines and Expectations

An RFP is not going to get you to a cloud deployment in a matter of weeks. You'll want to set realistic timelines within your organization as well as with your RFP respondents. Typically, the process looks similar to this:

Activity	Timeline
Develop and Write Your RFP	30-60 days
Vet with Cross Functional Stakeholders	30 days
Distribute Your RFP – Reply to Questions	30-60 days
Review and Rank Your Responses Against Matrix	30 days
Invite RFP Responders to Present	14 days
Narrow the Field	5 days
Discuss Pricing and KPIs	14 days
Review and Route and Sign Agreement	30 days

Developing Your RFP

Start by identifying who needs to be involved from your team. For a cloud services RFP, we recommend the lead be the CIO or someone from the office of the CIO. When working with sensitive data, such as PHI, it's important to get the Information Officer onboard with the approach from the start. You'll also want to include the Director of Infrastructure, and/or the Director or VP of IT or CTO. If you have a Director of Compliance or CISO, include them as well as your lead or Director of Security. Some organizations are now bringing on Directors of Cloud Strategy, and you'll want that position involved. You'll also need a finance component; if your CIO has budget control, he or she may serve in that capacity. Otherwise, a Chief Financial Officer will be good to help write and review some of the questions around your CapEx or OpEx considerations and depreciation tiers. Finally, be sure to include someone from project management who can ask questions around delivery timelines, Service Level Agreements (SLAs), Key Performance Indicators (KPIs), and other expectations.

It can take as long as you want to write an RFP, but we recommend setting a goal to have it written and reviewed in the same quarter, as public cloud capabilities, along with your requirements will change rapidly. There are suggested questions later in this document that you can use to begin to develop your RFP. Have your team work on a shared document so everyone's concerns are visible to the entire team. Have weekly check-ins with objectives/sections to discuss and resolve.

At the same time, you'll want to charge someone on your team with collecting the names of organizations you're going to reach out to. You may publicly post your call for proposals as well, but it's good to do some homework and find the top five to ten vendors that show promise. Have someone on your team browse their websites for key differentiators to inform your questions and enable you to compare areas of expertise in compliance, privacy, and security for healthcare. For example, because you work in healthcare and are issuing an RFP, do a search of cloud providers who are HITRUST certified and vow to settle for nothing less, as many of your end customers and vendors will require it themselves. This will save you time and trouble on the back end because many of the controls and safeguards you'll need in place to protect your PHI will already be assured by way of that vendor's HITRUST certification.

At a high level, here are some important items to expand upon in your RFP:

- Statement of your business objectives/goals in the cloud.
- Overview of your current state for that project or program.
- Overview of your current technical environment.
- Staffing areas of expertise and gaps so the respondent knows.
- Any workloads in the cloud already, i.e., DIY projects and on what platform.
- Platform preference, if you have one.
  - For example, ClearDATA offers our platform of solutions and managed services on AWS, Google Cloud Platform and Microsoft Azure. If our potential customers don't let us know which platform they prefer, we can look at their current state and business objectives and make suggestions for them.
- Demonstration of the vendor's/partner's expertise.

Questions to Include in Your RFP

Here are some more specific questions about security, privacy, compliance, and service level agreements any healthcare organization should consider incorporating into its RFP.

These are not comprehensive but will give you a good start in your evaluation.

Security Questions

- How do you vet new security vendors? Share details about your vendor assessment process.
- Do you have Business Associate Agreements in place with all of our security vendors that process, store, or transmit PHI? Ask even if it is an unlikely scenario like an application monitoring vendor, in which storing, processing, or transmitting PHI would be unlikely.
- Do you have a 24/7/375 Security Operations Center (SOC) offering? What is its makeup? Provide details regarding staffing, response SLAs locations, etc.
- What technologies do you use for, or along with associated MOP (method of procedure):
  - Vulnerability scanning,
  - Penetration testing,
  - Malware/antivirus,
  - IDS/IPS,
  - Availability monitoring,

  - Application monitoring,
  - SIEM (Security and Information Event Management),
  - Event and application logging,
  - Operation system and application patching,
  - Security monitoring; and/or
  - Device management.
- What is your documented process for day zero security vulnerabilities, both internally and externally?
- What is the Security response SLA?
- Does your cloud solution have a registry of cloud services along with its risk assessment?
- How many cloud services are tracked in the registry/ knowledge base?
- How is data encrypted within your solution, BOTH at rest and in motion? Please provide details.

Privacy Questions

- What is your incident management process? Attach documents that illustrate or describe the process in detail.
- Are usage logs sent off-premises for analysis? If so, how do you protect sensitive data (usernames and IP addresses etc.) within the logs?
- Are usage logs automatically ingested from their sources (proxies, firewalls, SIEMs, etc.)?
- Can your solution detect data exfiltration attempts? If yes, please describe how.
- What historical duration do you hold log data to provide visibility and analysis?
- Can we complete a penetration test?
- When do you disclose my secure data to other parties, and if/ when, how do you notify or consult my organization?

Compliance Questions

- Who are your third- party compliance assessors and what is their associated contact information?
- What compliance certifications do your organization hold?
- Can you send all relevant security and compliance certificates including SOC 2, SOC 2 Type II, HITRUST, and other applicable based on use case like PCI?
  - When was the last time each was tested by a third party?
- What are the key priority gaps that were identified in your compliance audits that your organization is working to address?
- What is the cadence of your third-party audits and who is involved from your organization?
- Describe your disaster recovery and business continuity plans, procedures, testing cadence, and recent results.
- Has your product been part of a product evaluation by a leading analyst firm (e.g., Gartner, Forrester?) Please provide details and a link to the report.
- Does your solution provide pre-built templates for IT teams to enforce policies required for compliance with HIPAA, GDPR, PCI DSS, HITECH, etc.?

Services and SLA Questions

- Please provide five references that are using your security, privacy, and compliance solutions.
- What are your response SLAs, based on severity (ITL aligned)?
- Do you have resolutions SLAs, based on severity (ITL aligned) and if so, what are they?
- How is your services team staffed (24/7/365 example, onshore/offshore, redundancy, locations)?
- How do customers open tickets (phone, email portal, etc., – list all) to get assistance and start the SLA clock?
- What service tiers to do you offer customers?
- Do you have different services offerings for different healthcare use cases (e.g., PHI, non-PHI, test, dev, etc.)?
- What professional services offerings do you have (e.g., cloud migration, data ingestion, DevOps, CICD planning and build out, etc.)

Issuing the RFP

Now you're ready. Before you issue the RFP, if you have contracts with analysts, such as Forrester or Gartner, be sure to gather their feedback to identify gaps in your requirement gathering and questions. Then, meet with your team and determine what questions you will entertain from respondents during the open period and decide who will be the person to take and respond to these questions in a timely manner. Make that evident in your RFP and align the team on a matrix for evaluating the RFP responses before you issue the RFP. Then, press send.

We recommend allowing 30-60 days for responses. The goal is to be as open as possible with respondents before the deadline date to get the most thorough and comprehensive view into what they can offer you. Once the deadline has passed, you'll want to cease any communication with respondents while in the initial review process, other than to inform anyone who asks that the RFP responses are under review and finalists will be contacted the week of (insert your date). Be certain someone on your team is assigned to collect the RFPs, log the date they were received, and begin to populate your spreadsheet or other tool/app with responses so you can align them to your matrix for a strategic and effective review.

Selecting Your Partner

After you review the responses, bring in your favorites and ask additional questions. This is also the time to have them expand upon on the answers to the questions in your RFP, having them cite examples of recent work that was similar. Check the references they provided.

Once you narrow the field and are prepared to talk KPIs and final pricing, the RFP response and your matrix go to the CIO or your legal counsel and the lead on the vendor side. Then, make your selection, sign your agreements, and prepare for your migration — or scaling if you are already in the cloud.

At ClearDATA, we provide industry-leading compliance, security, and privacy to hundreds of healthcare organizations, from some of the nation's largest hospital systems to small life sciences research firms. We will be with you each step of the way and can also point you to additional services and solutions that fill needs within your organization.

CLEARDATA™

ClearDATA.com | (833) 99-CLEAR

How can ClearDATA help?

ClearDATA is healthcare's largest managed cloud and security provider, protecting data in the cloud with proprietary technology and services — so you can operationalize your privacy and security and accelerate your digital transformation.

Speak with an Expert

MKT-0063, Rev. B, May 2023