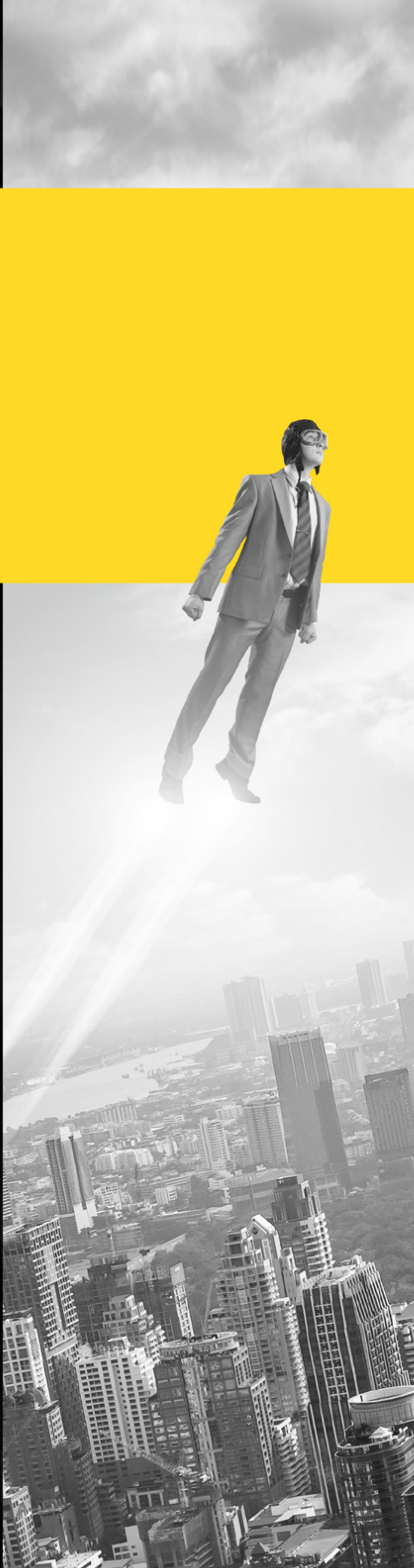
Health Tech's ULTIMATE GUIDE to the Healthcare Cloud



CLEARDATA™

Health Tech's Ultimate Guide to the Healthcare Cloud

Designed to address healthcare IT's unique challenges and offer solid solutions

As one of the economy's most **rapidly evolving** and **rapidly growing** market segments, Health Tech faces tremendous pressure to innovate at the speed of—well—the cloud. Financial pressures in the form of investors and funding just add fuel to the pressure cooker, leaving entrepreneurial IT teams seeking ways to get to market—fast and on budget.

While the cloud presents a powerful platform to address many health tech requirements, it doesn't come without its own set of challenges. That's where you can leverage a few simple insights to accelerate your intiatives and capitalize on the full potential of today's modern health cloud.

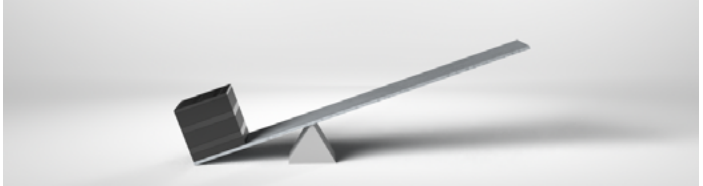
INSIDE

- ▶ Time is Money: Accelerate Time-to-Revenue and Eliminate Costs With the Healthcare Cloud
- ▶ How Compliance Should Fit Into Healthcare Tech's Go-to-Market Messaging
- ▶ Top 5 Tactics To Optimize Your Cloud Efficiency and Costs
- ▶ What is HITRUST Inheritance and Will Buyers Expect You to Have it?

Time is Money

Accelerating Time-to-Revenue and Eliminate Costs with the Healthcare Cloud

You are capable of doing anything—**but not everything.** My guess is that most of you have mowed your own grass and fix the occasional leaky faucet in your home. But what about when that shingled roof springs a leak? You could read a book on construction for dummies, or watch a plethora of YouTube videos. But there are only so many hours in the day and let's face it—you're not a professional roofer and there's only one of you. So, it's time to weigh your options. How can you leverage a roofer— or a Managed Health Cloud—to accelerate your project?



1. Force Multiplier

Even though operating with startup-sized resources can feel like a limiting factor at times, often these resource constraints produce remarkable ingenuity by founders. If you're in a position where your company is resource-constrained, one of the most critical steps you can take is to determine how to achieve maximum leverage. In other words, how can I deploy my capital to produce the highest impact?

Based on ClearDATA's experiences and prevailing industry estimates, it would require approximately seven full-time cybersecurity hires at an estimated cost of $1.6 million, just to form a skeleton crew who could start piecing together a program. Compound that with delays associated with hiring, onboarding, and program design and it's a costly proposition. For young health tech companies looking to disrupt and improve the healthcare industry, these costs and operational requirements can present a significant delay in time to market.

Partnering with a third-party managed cloud and defense specialist with HITRUST certification allows you to bypass some of the investment of time and money incurred when creating your own security program from scratch. In addition to the engineers, automation, and round-the-clock management of your security and compliance posture, you have access to fractional Subject Matter Experts—a call away for use when you need them.

2. Operationalized Security & Compliance

Early stage health tech companies have a mountain of work ahead of them to stand up a new application with a fledgling security and compliance program. Not to be overlooked, it will take you an average of six months to hire a basic team. It's critical that you research and maintain an intimate understanding of a multitude of complex healthcare regulatory frameworks. Simultaneously, you will also have to plan, acquire, implement, and build create security processes and tooling adequate to protect your business. Keep in mind that standards, regulations, and threats all evolve continuously, and maintaining a secure environment is a never-ending work in progress. The end result is spending unnecessary amounts of your company's limited capital on foundational security and compliance processes.

Should you choose to partner with a third party cloud or cybersecurity company, you will benefit from a complete playbook for highly secure and compliant business operations from day one, maintained and researched continuously, with dedicated teams on hand around the clock to actively defend, adjust, notify, and consult to keep your business operating smoothly.

For health tech companies that are just starting out, inheriting operationalized security and compliance processes is one of the most effective ways to save time and money you would have spent building out your own processes from scratch—with all the liability on your shoulders.

3. Access to Healthcare Threat Intelligence at Scale

When you operate in the healthcare industry, your company is going to be the target of ransomware and other cybersecurity attacks from sophisticated attackers all around the world. According to the Verizon Data Breach Investigation Report for 2021, healthcare organizations were the victim of 472 confirmed data breaches due to cybersecurity vulnerabilities. Because of the exponential value of sensitive data and protected health information (PHI) on the black market, it's simply a matter of time before your cybersecurity defenses are tested.

If your company is operating as an island, without deep industry-specific threat intelligence and insights about recent cybercrime events and predictive patterns, you're going to be operating in a reactive state to emergent threats.

As a result, one of the major value propositions for digital health companies that consider a third party engagement, is that your company gets access to healthcare threat intelligence at scale. Because a third party cloud security company can augment your individual experience with that of a broad swath of industry entities, analyzing and creating insights real-time.

Most importantly, the third party company can distill the most effective defense strategies to your healthcare IT company so you can see around corners, protecting your customers' data, their patients' data, and your own reputation.

4. HITRUST Inheritance

One of the most non-negotiable certifications required of health tech applications is HITRUST certification—particularly if your target market includes providers. But attaining HITRUST certification is highly laborious, requires immense investment of personnel hours and expertise, and can take upwards of six months and hundreds of thousands of dollars to achieve. It's often a gating item that you need to fast track on the road to marketability. So, how do you get that party started and get your application on the market faster?

Some HITRUST-certified organizations—like ClearDATA—offer a HITRUST inheritance program. The HITRUST CSF Inheritance Program simplifies the process of gaining HITRUST Certification for customers. By working with a partner, customers can reduce the required testing and associated costs for inherited controls in a fully automated manner, leveraging their HITRUST status to simplify their own CSF Assessments and manage the daunting task of securing their sensitive data (PHI). While each certification is unique, you may be able to inherit some controls from almost all of the 19 Domains, thus significantly reducing your time and costs to certification (and to revenue).

Pick the Right Partner

Partnering with an experienced third party company gives you access to ready-to-implement automation software and an expert team, steeped in programmatic compliance and defense. There's no need to potentially create your own automation software, go through a lengthy trial process with multiple automation software products, or go through a costly hiring process to recruit talent for your team. The scope of threat intelligence gleaned from direct experience and analytics across hundreds of healthcare organizations is impossible to replicate in a timely manner. With a third party, you immediately gain value from the breadth of their portfolio and experience.

Because, at the end of the day, you need your application on the market as soon as possible, not hung up in the operational abyss that can occur when you build critical support functions from scratch. The sooner you stand up your cloud, defense, and compliance infrastructures, the sooner you can start collecting revenue and impacting patient lives.

How Compliance Should Fit into Healthcare Tech's Go-To-Market Messaging

For any organization in the healthcare ecosystem, privacy, cyber defense and compliance aren't just priorities; they are table stakes. This is especially true for organizations that are considering moving protected health information to the cloud. At a time when the value of patient data leads the black market, breaches are reaching record levels, and regulatory requirements continue to evolve, healthcare buyers want to know one thing before they even consider a new technology solution:

Will it keep my data safe and my organization compliant?

Therein lies the challenge, and opportunity, for digital health companies. Whether approaching prospects in the provider, payer, or life sciences markets, healthcare tech organizations need to be sure compliance and security are at the core of their solutions. More importantly, they need to be able demonstrate the extraordinary measures they have taken to meet these critical needs. If a buyer feels they can trust you with their data, they are more likely to trust you with their business.

Here are a few tips for fitting compliance and security into their marketing messaging: what to avoid, what is important, and the value of taking a "show don't tell" approach.

What Buyers Don't Want to Hear

Oversimplification

While healthcare organizations want to know that a tech company prioritizes security, privacy, and compliance, they don't want to hear blanket statements that lack empathy or minimize what's at stake. Oversimplified comments such as, "We get it," "We understand HIPAA," and "Don't worry" are red flags for buyers, especially during the sales process.

One-Size-Fits-All Generalization

Healthcare organizations don't want empty promises; they want assurance that a tech company has taken the time to fully understand the challenges those buyers face. For example, they want to know their vendors understand the hard and soft costs of a security breach, the complexities of daily compliance tasks, and even more importantly, how they are addressing these types of obstacles.

Irrelevant Information

Buyers also don't want to read or listen to a long list of technology features. While it is tempting for a healthcare IT company to tout the technical bells and whistles of its latest solution, buyers are far more interested in learning about how the solution will solve a real problem they are facing. Technological advancement means little to a healthcare organization unless it makes their day-to-day jobs easier and faster.

For example, while a tech company might highlight the fact that their solution offers two-factor authentication to ensure data privacy and security, a provider may actually view this as a stumbling block. If a doctor's goal is to see as many patients as possible in the shortest amount of time, having to go through two-factor authentication every time he or she wants to access patient data is a limiting factor that slows down efficiency and actually works against his or her business needs.

What Buyers Do Want to Hear

Tailored Solutions

The key is for tech companies to communicate the ways in which their solutions cater to the unique needs of healthcare organizations, both from a security and compliance standpoint as well as a business performance standpoint. This means getting into the head of the user: What day-to-day problems does the solution address? Will it create new obstacles? Why is the learning curve worth the effort? If a critical issue surfaces, how quickly will it be addressed?

Across the board, healthcare organizations want technology partners to show—not just tell—them the steps they have taken or are willing to take to keep their business safe and thriving. Earn your prospective buyers' confidence by addressing the following:

1. **Demonstrate your commitment to compliance.** Walk the buyer through what you are doing to safeguard the buyer's data, as well as the internal procedures you follow to maintain security and privacy within your own company. This is a prime opportunity to share if your company is HITRUST certified or if you are working with a partner that has this certification. Other details to share include the timing of certifications, relevant audits, renewal plans, response time to security incidents and regulation changes, and use-case examples of how these issues have been handled in the past.

2. **The risks you are willing to share.** Although no one wants to talk about security incidents or noncompliance, buyers do want the assurance that partners will have their back if these situations arise. Too often the financial burden and marketing backlash of data breaches and audit failures fall solely on the healthcare buyer, jeopardizing their business, their reputation, and patient safety.

   Buyers want to know that, when applicable, vendors will share part of the risk and responsibility if something goes wrong. For example, some tech companies spell out in the BAA the risks it is willing to share with buyers, either financially or from a marketing perspective, and many provide a detailed crisis management plan.

3. **The resources you will make available to them.** Service is a critical part of any business relationship, especially when it comes to risk-averse industries like healthcare. Providers, payers, and life science organizations want to feel confident that they will be fully supported before, during, and after the sales phase. If you have ongoing access to their data, they will want to have ongoing access to you.

   Providing potential buyers with a list of contacts, tools, and resources that will be available to help them speaks volumes about the level of service your company can deliver throughout the business relationship. In some cases, this may require bringing in third-party partners to fill in any gaps that fall outside of your company's core competencies.

Delivery is Critical

It is also important to remember that how health tech organizations deliver the message is just as important as the message itself. The way a vendor treats a potential buyer sets the tone for the business relationship and is the first step toward building trust. There are several strategies healthcare companies can take to ensure their delivery is effective, but the overall aim should be to exhibit your company's customer experience competencies throughout the sales process. Put simply: Actions speak louder than words.

In general, healthcare organizations are looking to work with partners that demonstrate two key values:

1. **Customer-focused.** Research shows that how a buyer feels impacts their purchasing decision. From day one, a buyer should feel like a priority, not just another sales target. This type of support is especially important to healthcare organizations that are nervous about moving into new, uncharted waters like the cloud.
2. **Responsive.** How a company behaves up front usually indicates the level of response a potential buyer can expect throughout the business relationship. For example, if a vendor can't be responsive for basic interactions like phone calls and emails, how can it be trusted to react quickly in the midst of a crisis?

A Trusted Foundation

In the end, today's healthcare organizations want to feel understood, prioritized, and safe before taking a chance on a new technology solution or service. By prioritizing security and compliance and taking a "show don't tell" approach, healthcare IT companies can garner the trust of healthcare organizations and begin building the foundation for successful, long-term business relationships.

Top 5 Tactics to Optimize Cloud Efficiency and Costs for Healthcare Tech

Once your application is launched in the cloud, there are a number of highly effective tactics your Chief Technology Officer or development team can implement in order to optimize your cloud efficiency from both a performance perspective and a cost perspective.

#1 Balance Your Services

If you are working in an Infrastructure-as-a-Service, or IaaS context, you are encouraged to examine the choice of VM instances used. Because there are different architectures of the instance families available, this means you will have numerous options for selecting the right balance of performance characteristics. You could opt to prioritize high amounts of memory, high CPU power, or even high networking throughput. It is especially important to see if you have existing workloads that have run for a while; new instance families might have come out since your initial setup that provide enhanced performance for the same cost. Many times it's easy to move existing workloads to newer more capable instance families with little downtime. This is true of all cloud providers, but especially true of Amazon Web Services (AWS). On Microsoft Azure and Google Cloud Platform (GCP) it may be easy to simply add new resources to existing VMs.

#2 Environment Visibility

Also relevant for IaaS: your IT team can't track down performance problems if you can't see critical operating system metrics. As you operate in a cloud environment, make sure you are monitoring the critical VM metrics of CPU utilization, memory utilization, disk throughput, and space utilization. We recommend you track average and peak values over time to identity usage trends, and ultimately determine where problems lie. Identifying these problems will enable your team to improve operational efficiency immediately.

#3 Storage & Servers

As part of your IT buildout, you will have to weigh the advantages and disadvantages of using SSD vs mechanical disks. Each type of storage has its own pros and cons. For the purposes of cloud computing though, AWS instance storage volumes can be very fast. Oftentimes, these instance storage volumes can be much faster than Elastic Block Store (EBS) volumes. However, instance storage volumes should be specifically used for caches and other temporary storage that is not backed up. The instance storage volume can operate much faster, but they will be emptied after EC2 instances are stopped and restarted. As a result, we recommend you allocate instance storage volumes for situations where you need temporary storage that can operate very quickly. If you want to store data for longer periods of time, encrypt it, and preserve it through instance stops and terminations, then EBS volumes would be ideal.

#4 Autoscaling Architectures

A highly effective tactic to optimize cloud performance and cost, even as loads may rise and fall over time, is shifting to autoscaling PaaS and FaaS Architectures. These designs are built from the ground up to scale more efficiently as loads increase and decrease, and are a great tool in any IT leader's toolbox.

#5 Serverless Integration

For any database applications operating in AWS, we recommend that you consider autoscaling/serverless cloud-native database architectures such as Aurora Serverless. Aurora Serverless is an AWS product that offers the same scaling advantages as PaaS and FaaS computing capabilities discussed in the previous point. You're able to specify the desired database capacity range and connect your applications so you are ensuring optimum performance without the need for human supervision. Without autoscaling technology, your IT team may become bogged down dealing with variable computing loads and is unlikely to operate nearly as efficiently as an automatic application.

▶ Creating highly effective cloud architecture can be a time-consuming process, and it's not one that you want to start over if you realize your foundational decisions were sub-optimal. If you're currently building out cloud architecture or want to make sure you are extracting maximum performance from your cloud environment, reach out to the ClearDATA Professional Services team and learn the most cutting-edge cloud solutions.

HITRUST

What is HITRUST Certification? Will your buyers expect you to have it?

Among all the things healthcare companies expect of you as they move their patients' protected health information (PHI) out of internal data centers and into the cloud, **Health Information Trust Alliance certification (HITRUST) is one of the most important**.

That's because in an age of unprecedented security risks and a seemingly neverending list of regulatory requirements, HITRUST certification is like a Good Housekeeping seal of approval. It's a way of not only securing your customers' sensitive patient data, but also ensuring that they remain compliant with all the regulations affecting the healthcare industry. Let's take a closer look at HITRUST and why it's so important.

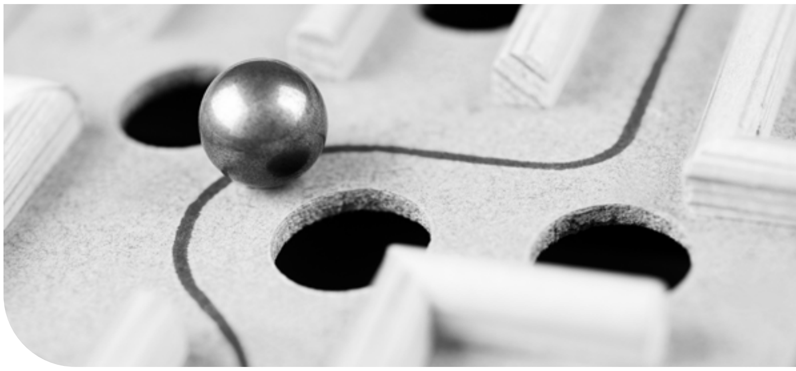
What you need to know about HITRUST

HITRUST was born out of the belief that information security and privacy should be a core pillar of the broad adoption of health information systems and exchanges. Working in collaboration with healthcare, business, technology, and information security leaders, HITRUST established the HITRUST Common Security Framework (CSF), a certifiable framework for organizations that create, access, store, or exchange personal health and financial information.

Fundamentally, HITRUST is an information security framework for the healthcare industry. It brings international, federal, state, and third-party regulations and standards together into a holistic set of controls designed to protect healthcare data. More specifically, it provides a clear and measurable benchmark for identifying hosting and cloud computing vendors that meet the highest standards of HIPAA compliance, thus reducing your risk to the lowest level possible.

But it doesn't just ensure HIPAA compliance. With HITRUST certification, you can more easily comply with PCDI-DSS, ISO 27001, COBIT, NIST and FTC, as well as the growing number of state laws. As a result, rather than being concerned about whether your third-party partners have met the many standards individually, HITRUST certification ensures that your partners are compliant with all of them, while eliminating the variability in the definition of acceptable security requirements.

Now that we know what HITRUST is, let's look at what getting certified entails →



The Path to HITRUST Certification

To achieve HITRUST certification, you must successfully demonstrate that your organization meets all of the controls in the CSF required for the current year's certification. Not only that, you must do so at the appropriate level required for your specific organization based on your responses to the MyCSF self- assessment tool requirements statements. In addition, you must achieve a rating of three or higher on HITRUST's scale of one to five for most control domains documented in MyCSF.

Practically speaking, this is a lot easier said than done. Organizations that are well-prepared require anywhere between six and nine months to get certified. Meanwhile, for some organizations, the process can take a year and a half or more and cost several million dollars. Having said that, it's often worth the effort. Not only does HITRUST certification bring prestige to organizations, it's also something that healthcare tech buyers increasingly expect.

Payers and Providers Trust in HITRUST

With HITRUST CSF certification, you can signal to your business partners and other third-parties that you've made protecting sensitive information a priority. Not only that, it's a clear indication that you have essential security and privacy controls in place, and that your management team is committed to privacy and information security. As a result, a growing number of healthcare organizations, including Anthem, Health Care Services Corp., Highmark, Humana, and UnitedHealth Group all require certification.

If you want to do business with payers and providers, a HITRUST certification is almost always non-negotiable. Not only that, being certified can also help shorten sales cycles by streamlining the diligence process and making conversations with Chief Information and Security Officers easier.

Alternatively, companies that want to accelerate their HITRUST journey can partner with providers that allow for HITRUST inheritance. In that way, they can adopt their provider's scores on approved controls, making the process much less onerous and saving considerable time and money. It's also possible simply to work in a HITRUST environment. In such instances, your company will not have gone through all of the hoops necessary to become certified but will still get many of the benefits HITRUST brings.

The bottom line is, if you're unsure how best to approach HITRUST, the best way to move forward is simple: **Partner with a cloud platform provider who understands healthcare and can provide assistance in, or alternatives to, HITRUST certification.**

CLEARDATA™

ClearDATA.com | (833) 99-CLEAR

How can ClearDATA help?

ClearDATA is the trusted partner, protecting healthcare data in the cloud with proprietary healthcare technology and services—so you can operationalize your privacy and security and accelerate your digital transformation.

Speak with an Expert