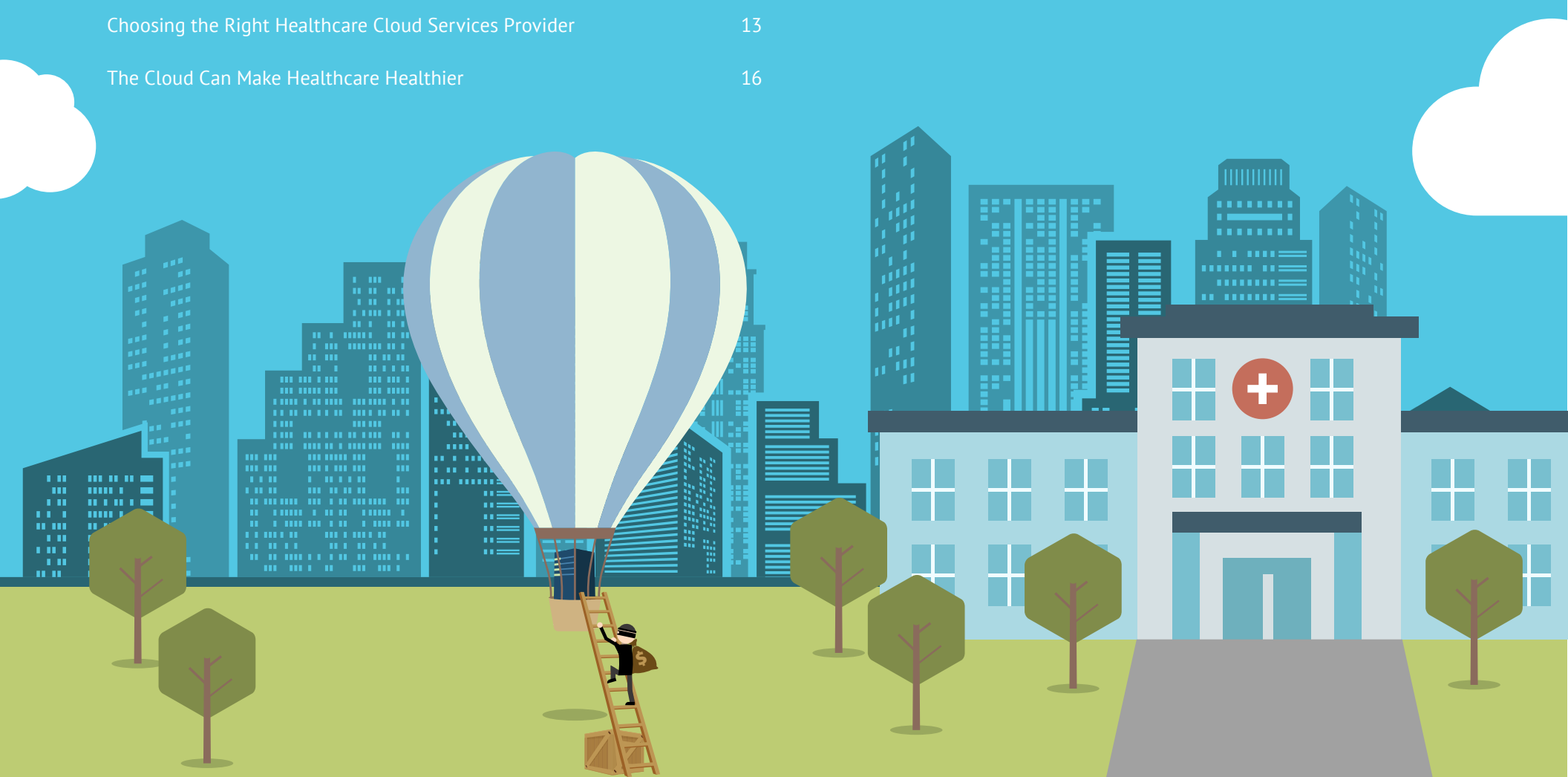
The Safest Place for Healthcare Is in the Cloud

Entrust PHI Security to a Healthcare Cloud Services Provider

Table of Contents



Introduction

While data security is a top priority for IT professionals in every industry, this is especially true for those supporting healthcare organizations. Besides the fact that healthcare is one of the most highly regulated industries requiring stringent security and privacy safeguards, data thieves are becoming increasingly sophisticated in their efforts to infiltrate data centers run by healthcare organizations. Several recent and notable breaches have shown just how effective cybercriminals are at gaining access.

Protected health information has more value on the black market than credit card numbers alone because it can be used by identity thieves to obtain pharmaceuticals and medical care. In addition, health organizations are vulnerable targets because they are often slower to adopt the latest security measures, such as keeping personal information in separate databases that could be inaccessible in the event of an attack.[1]

What's the prevailing reason why the healthcare industry is slow to adopt the cloud? Fear. According to a recent HIMSS survey, security concerns are cited as the top reason healthcare organizations don't currently use cloud services (62%), as well as why some don't plan on using cloud solutions in the future (44%).[2] IT professionals in healthcare agree, according to a recent Spiceworks survey in which security was the top reason cited (58%) for healthcare organizations not yet adopting the cloud.[3]

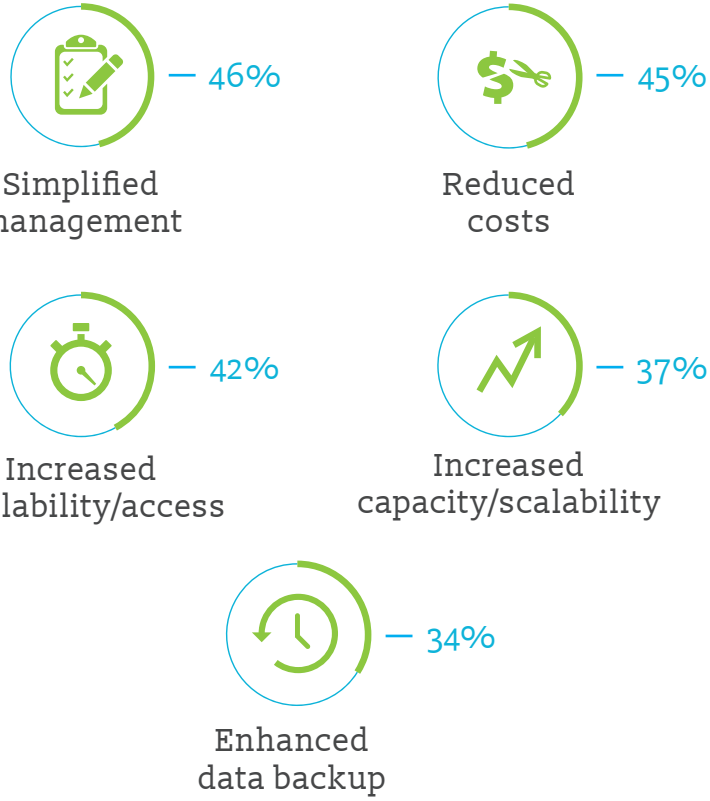
But the truth is, healthcare organizations—already resource-constrained—need to be continuously investing in advanced security measures to protect their PHI. Those that don't may pay an even steeper price.

Chapter 1

A Better Way to Protect your PHI

From the physical security of on-site servers and individual devices to the virtual security of private patient data, healthcare IT professionals have a lot to think about.

In the Spiceworks survey, IT professionals reveal the top advantages of using cloud services in the healthcare industry:[3]



The Spiceworks survey also revealed that just 45% of IT professionals in healthcare are currently using cloud services.[3] What about the 55% who aren't?

Healthcare IT professionals need to know they can leverage all the benefits of the cloud—securely. The key? Choosing the right cloud solution to manage even the most stringent security regulations—one that also provides IT pros with peace of mind.

The Adoption of Cloud Services:

45% of surveyed healthcare IT professionals use cloud-based services today[3]

20% of surveyed healthcare IT professionals plan to use cloud-based services in the next 12 months[3]

But what about everyone else?

Chapter 2

Why the Cloud Can Seem Like a Scary Place

The traditional approach to healthcare computing is in-house and on-site. Software applications run on an infrastructure built and maintained by the organization. Larger organizations may have data centers to centrally manage and store sensitive data, while smaller organizations may have servers in their local offices. In the traditional model, the data stays with the organization, and IT professionals have complete control over the data and its security.

When a healthcare organization uses the cloud, IT professionals must trust sensitive healthcare data to the cloud provider and its resources. They lose direct control over the data. This may seem like it would increase security risks… but in truth, there are huge security benefits in a cloud-based computing model.

Top considerations when deciding to move forward with a cloud services provider:[2]

Security issues, such as the physical or technical security of cloud services providers

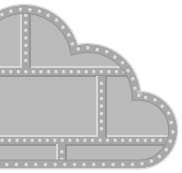
A cloud services provider's willingness to enter into a Business Associate Agreement (BAA)

Addressing Five Common Cloud Myths

Even the most knowledgeable healthcare IT professional may have doubts about cloud security. The following myths are pervasive, and what you don't know can hurt you—especially in heavily regulated healthcare environments.

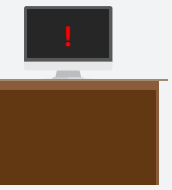
1. The cloud is not secure enough for healthcare.

Data shows that cloud-based systems are actually more secure than their on-premises counterparts. The reason? Better safeguards in the cloud.



2. All cloud-based infrastructures are created equal.

Healthcare-specific cloud infrastructure may include some common cloud components. However, it goes *much* further to protect PHI with purpose-built systems that follow stringent healthcare data retention policies.



3. Data in the cloud is more vulnerable to hackers.

Data in the cloud is less susceptible when it is properly encrypted and secured. HITRUST-certified vendors undergo a rigorous certification process to ensure the highest healthcare data security.

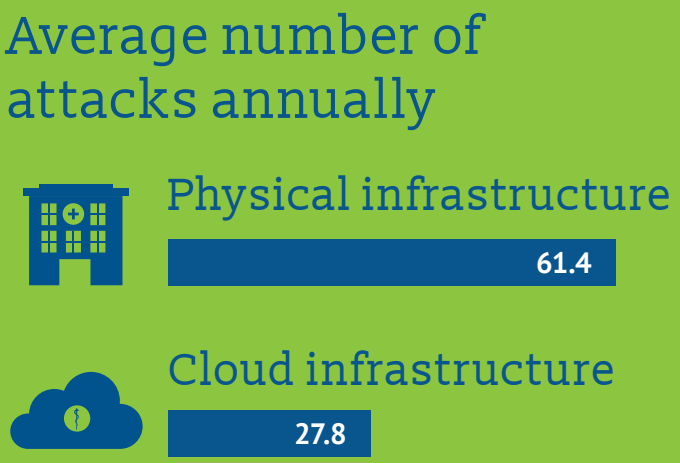
4. Data in the cloud is accessible to other organizations using the same cloud.

Cloud providers take every precaution to secure data. A healthcare-specific cloud solution will ensure the organization's data is isolated from other organizations' data at all stages.

5. Data that resides in the cloud cannot be controlled or mined by providers.

Healthcare IT pros can ensure they have control of data in the cloud by extending internal controls that they already trust into the cloud. Any cloud environment should allow them to maintain an auditable chain of custody for their data.

On-premises users experience an average of 61.4 attacks per year while cloud customers experience an average of only 27.8 attacks annually.[4]



Chapter 3

How Healthcare Organizations Use the Cloud

Some healthcare organizations are already using the cloud for certain functions. More than half host clinical applications and data in the cloud today, and nearly 47% use cloud solutions for health information exchange. And about 42% host human resources applications and data in the cloud, and use the cloud for backup and disaster recovery.[2]

Even more expect to use cloud services more in the future. By 2020, 80% of healthcare data will "...pass through the cloud at some point in its lifetime, as providers seek to leverage cloud-based technologies and infrastructure for data collection, aggregation, analytics and decision-making," according to IDC.[5]

According to the HIMSS survey, over 40% of healthcare organizations plan to use cloud services in the future to host archived data. Nearly 32% plan to use the cloud to host operational applications and data, and 31% plan to use cloud solutions for backups and disaster recovery.[2]

> By 2020, 80% of healthcare data will pass through the cloud at some point in its lifetime.[5]

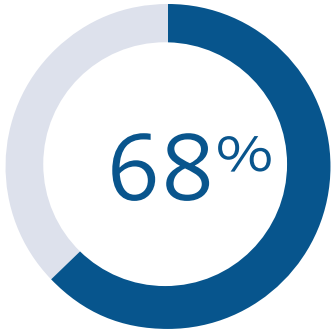
Why Healthcare IT Professionals Are Adopting the Cloud

One reason IT professionals in healthcare are moving toward cloud is the cost; cloud solutions are lower cost than maintaining current IT maintenance costs. This is why, according to a recent Spiceworks survey, 49% of healthcare organizations are adopting or considering cloud services. Forty-six percent are doing so due to the need for an on-demand, scalable, always-on solution, and almost 40% expect more robust disaster recovery.[3]

Today, a whopping 53% of healthcare employees use three or more devices for work.[6] Mobile device security is becoming more and more critical, and the mobile security tools IT pros have in the cloud are becoming more important.

As if that weren't serious enough, more security breaches actually occur from employees losing their devices than from hacks. In fact, 68% of all healthcare data breaches since 2010 were due to device theft or loss.[7]

Another reason IT professionals are moving to cloud? To keep up with the growing requirements in the healthcare organizations they serve.



of all healthcare data breaches since 2010 were due to device theft or loss.[7]

Finding Safety in Healthcare-Focused Cloud Providers' Security Measures

Not all cloud service providers are created equal. A suitable cloud provider for healthcare environments will have multiple layers of security measures in place. Most of those measures fall into seven categories: physical, server, network, application, data, devices, and users. Creating a properly secured healthcare cloud environment requires the hardening of security at each of these layers.

IT professionals may expect this level of security with most cloud solution providers—and many cloud providers also have staff that specialize in security, privacy, and other areas of concern for highly regulated industries—but healthcare-exclusive cloud solutions will have even more stringent and industry-specific security in place.

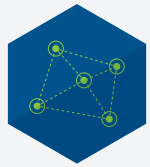
7 Layers of Security

Physical

To physically secure data, it must be stored in top tier data centers with 24/7 perimeter sensor-monitoring and badged or biometric entry into secure areas.

Server

Security at the server level includes file integrity monitoring, patching, role-based access controls and SIEM.



Network

Network security includes enterprise-grade hardware, advanced firewall configuration, SSL VPN security, threat management response and intrusion detection/prevention.

Application

Security at this layer means data encryption (at rest and in transit), anti-virus protection, patching, two-factor authentication, malware protection and log management.

Data

To secure data, cloud providers must offer backup, at-rest and in-transit encryption, retention, destruction, archiving, SIEM and lifecycle management.

Devices

Device security includes mobile and medical devices, as well as BYOD. This is a huge challenge for internal security because many devices are outside IT's control.

User

Security at the user layer includes two-factor authentication, social engineering and hacking education, policies related to passwords and BYOD, and corporate policy.

Chapter 4

Becoming a Smart Cloud User

Beyond the rigorous security measures healthcare cloud service providers offer, there are other important benefits to help IT professionals safeguard PHI:

Offsite backup and disaster recovery

When PHI is secured in the cloud, IT professionals can rest assured that it's protected from natural disasters, fire, water damage, vandalism, accidents and other factors that could damage the organization's physical infrastructure. Healthcare IT professionals can securely access the organization's data anytime, from any place.

Platform hardening

A cloud platform often enables more automation of security management activities like configuration control, vulnerability testing, security audits and patching.

Resource availability

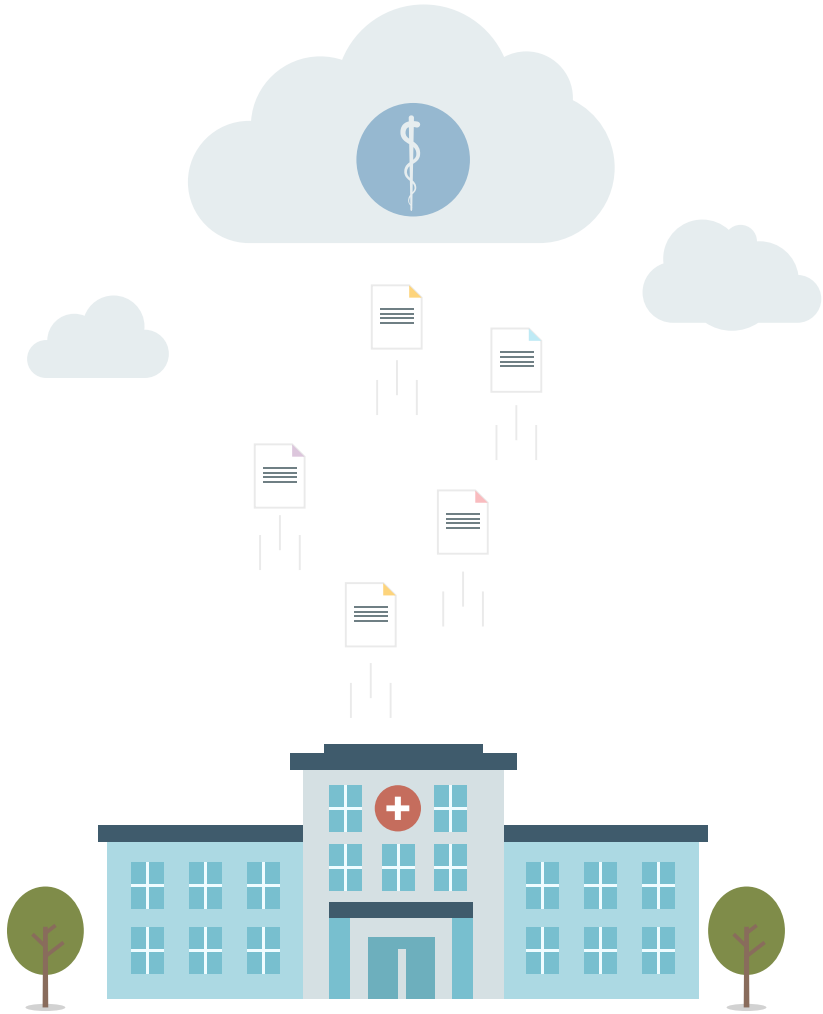
On-demand resource capacity provides greater resilience when organizations face increased service demands. It enables greater business agility, reduced project ramp times and endless ability to scale infrastructure while paying only for what is used.

Mobile device security

The use of mobile devices by healthcare practitioners has become an essential element of timely, effective patient care—however, lost or stolen devices is the number one cause of PHI breaches. Cloud technology gives practitioners secure, immediate access to patient data without storing data directly on the device.

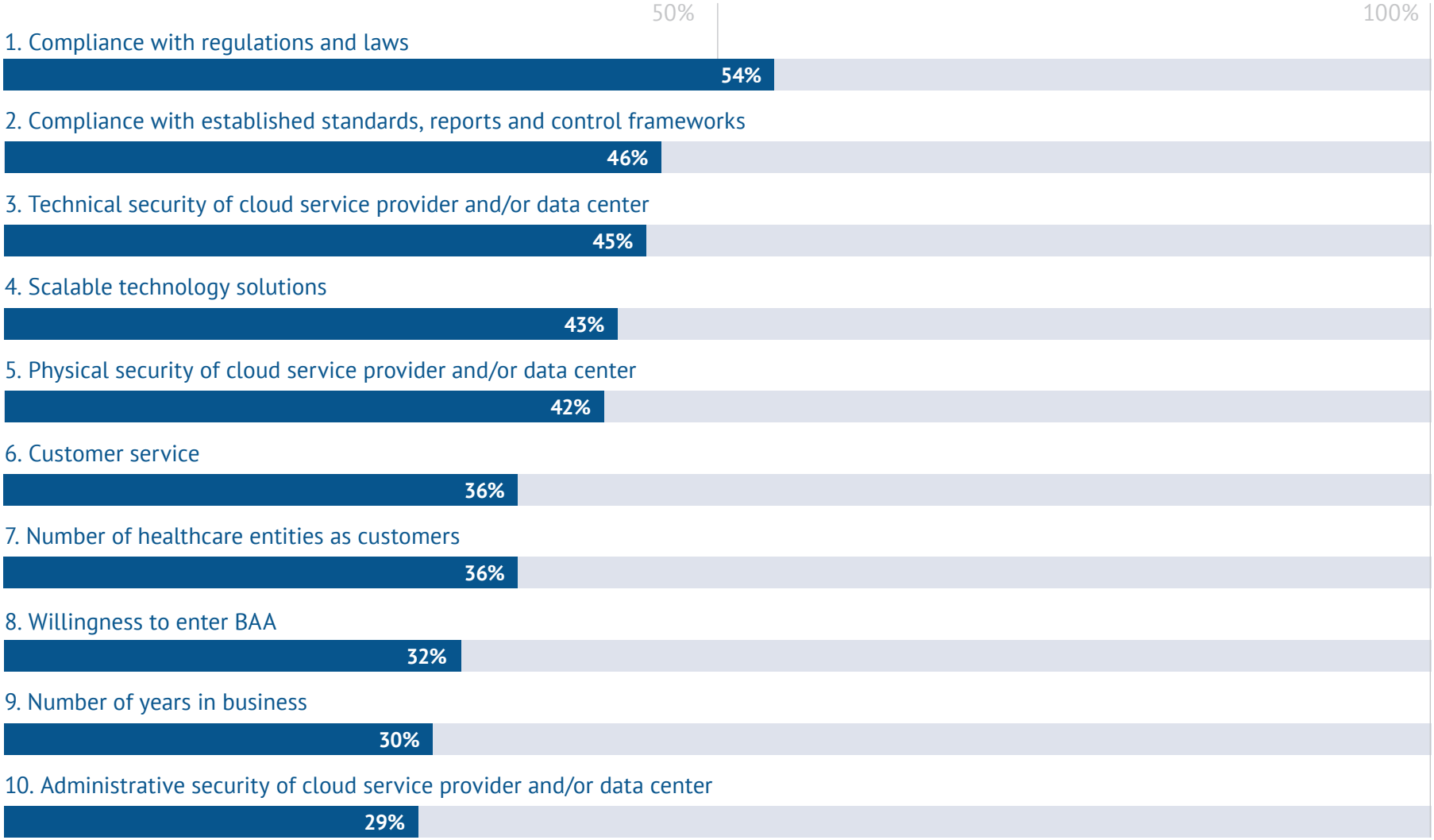
Chapter 5

Choosing the Right Healthcare Service Provider



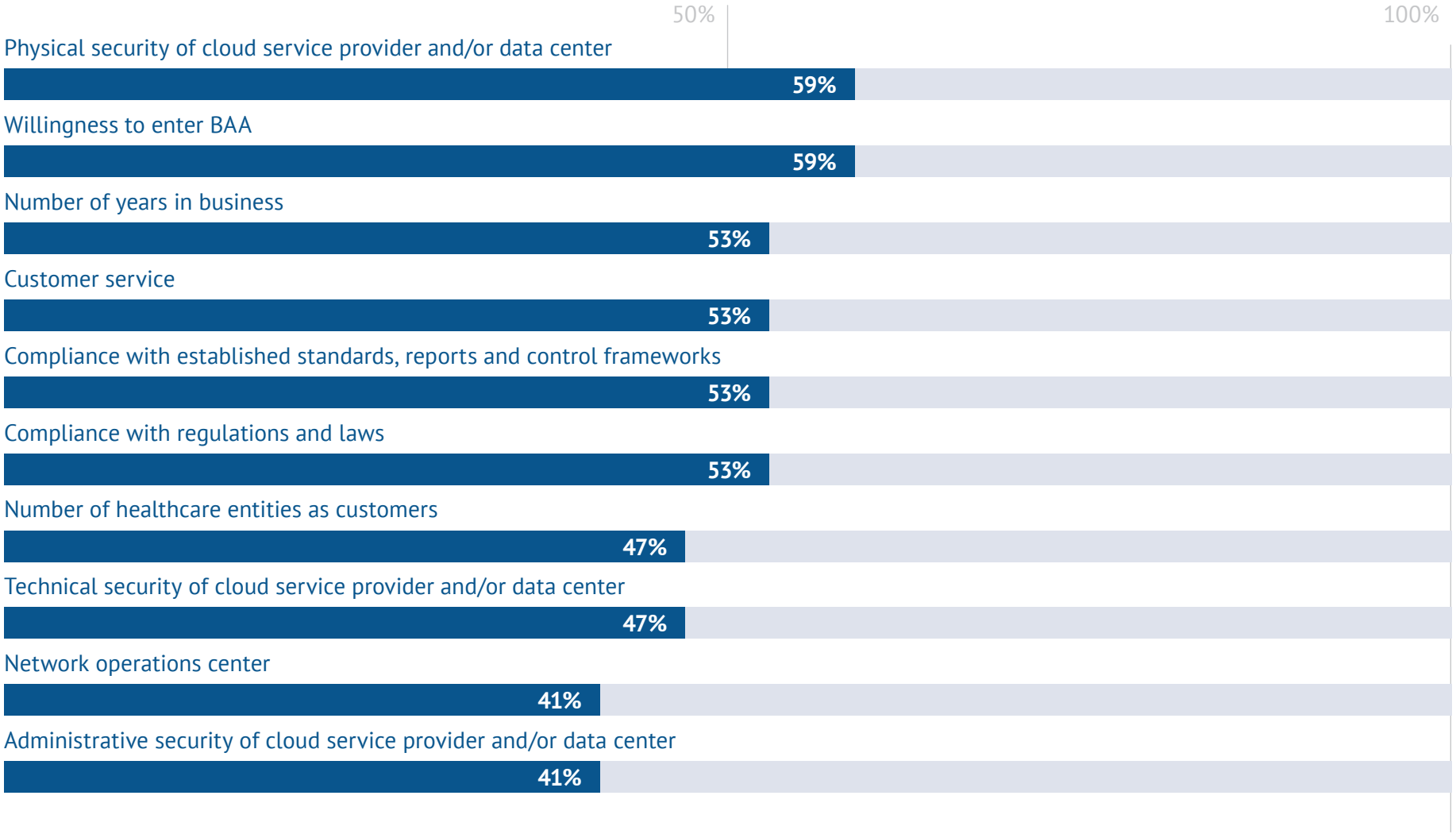
Top factors considered when evaluating a cloud services provider[3]

A healthcare-specific cloud solution provider will easily check all items off this list for IT professionals.



Top considerations for future cloud usage

When looking into the future, the picture changes a bit. According to the HIMSS survey, when evaluating future use of the cloud, healthcare organizations still value security, compliance and willingness to enter into a BAA. But they value customer service and the number of years in business quite a bit higher.[2]



What does this mean for healthcare IT professionals who are considering the cloud for their organizations? It means that choosing a healthcare-focused solution provider with experience and great customer service will benefit their organization now and into the future as their needs continue to evolve.

The right cloud solution can provide healthcare organizations the benefits of cloud computing while protecting sensitive patient data and optimizing operations. A cloud provider specializing in healthcare can ensure the highest level of security and compliance for this data-sensitive industry.

The Cloud Can Make Healthcare Healthier

The ClearDATA HealthDATA™ Cloud Platform is the only healthcare-exclusive cloud in the world, and combines the most advanced cloud technology, information security and performance. Our managed and professional services deliver increased data security and peace of mind to healthcare IT professionals and the organizations they support.

ClearDATA can address all your concerns.

ClearDATA
SECURE • HEALTHCARE • CLOUD

Learn more now

ClearDATA

SECURE • HEALTHCARE • CLOUD

Sources

[1] Healthcare data security: Is cloud encryption alone enough?," *Logicworks*, February 16, 2015. http://www.cloudcomputing-news.net/news/2015/feb/16/healthcare-data-security-is-cloud-encryption-alone-enough/

[2] "2014 HIMSS Analytics Cloud Survey," *HIMSS*, June 15, 2014. http://www.himss.org/ResourceLibrary/genResourceDetailPDF.aspx?ItemNumber=41958

[3] 3 Spiceworks survey of 100 U.S. IT professionals in healthcare, *on behalf of ClearData*, January 2015.

[4] "Removing the Cloud of Insecurity: State of Cloud Security Report," *Alert Logic,* Spring 2012. https://www.alertlogic.com/wp-content/uploads/alertlogic%20state%20of%20cloud%20security%20spring2012.pdf

[5] "IDC FutureScape: Worldwide Healthcare 2015 Predictions," *IDC Health Insights*, November 12, 2014. https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&eventid=857469&sessionid=1&key=0139B720D68E9462F050E955449F0648&sourcepage=register

[6] Statistic from Skyhigh Networks. http://www.forbes.com/sites/danmunro/2014/09/01/over-90-of-cloud-services-used-in-healthcare-pose-medium-to-high-security-risk/

[7] "The 2014 Healthcare Breach Report," *Bitglass*, 2014. http://pages.bitglass.com/healthcare-breach-report.html