Ping Identity

Beyond Compliance:

Using IAM to Surpass the Healthcare Interoperability Status Quo

How Healthcare Business Can Thrive in a Tech-Driven Future

WHITE PAPER

Healthcare organizations today are faced with many serious challenges: tight budgets; workforce shortages; well-funded competition from new entrants; legacy systems and IT environment complexity; breaches and fraud; and regulatory mandates. Unlike any other time in history, digital technologies are now critical to address these challenges and more. According to Grand View Research,[1] "The global digital health market size was valued at US $211 billion in 2022 and is projected to grow at a compound annual growth rate (CAGR) of 18.6% from 2023 to 2030."

The adoption of digital technologies in healthcare has fostered an increasingly connected and sophisticated healthcare customer (patients and members). For example, patients now expect to participate in healthcare decisions, access an expanding array of online services, information, and receive real-time support. They also want to make appointments; attend telehealth visits; pay their bills; get care reminders and tips; and see that their prescriptions are ready for pickup all from a single, user-friendly app.

According to PwC:

49%
of provider executives say patient experience is a top strategic priority over the next 5 years.

81%
of payer executives say their company is investing in technology to improve member experience.

91%
of pharmaceutical executives think that customer self-management will increase over the next 10 years with pharmaceutical companies' patient engagement services.

Furthering the momentum of digital healthcare, many customers also tie their unique, secure digital identities to wearable devices and digital services. These devices and services can be authorized to collect health data on their behalf and share it with other authorized users, such as providers, family members, payers, retailers, and researchers. Wherever the customer goes, their digital identity follows.

> "By 2030, the market size of patient engagement solutions – which includes wearables, educational resources, and mobile apps – is estimated to reach US $74.28 billion, up from US $13.42 billion in 2021."
>
> **– Healthcare Transformers[2]**

But for this type of integrated digital healthcare to succeed, customers must feel confident that their data is safe when they share it — otherwise, they won't. And without it, effective care can't be provided. This makes customer confidentiality critical.

Providers, workforces, (such as employees and contractors), and partners are also demanding better digital experiences. Overburdened with administrative tasks and manual processes, they seek out organizations that offer user-friendly digital solutions that reduce friction, improve care outcomes, and make their lives easier.

93% of physicians feel digital health tools are an advantage for patient care.

– AMA[3]

The trends and statistics previously mentioned illustrate that healthcare leaders must continue their digital transformation to meet the demands of today's savvy customer and overburdened providers and workforce. Secure, unified digital health ecosystems are the vehicle to meet these demands. They result in more informed care, streamlined operations, improved outcomes, differentiated business, and reduced costs.

"Health systems are looking to build stronger, more continuous relationships with their customers that enable growth. Investments in virtual care, analytics, and CRM tools can build better relationships and drive growth…"

– PwC[4]

Digital health ecosystems are a network of interconnected digital services. They need to accommodate any type of user to support a variety of digital healthcare use cases and innovation. User types not only include customers, providers, workforces, and partners, but also connected IoT/IoMT (Internet of Medical Things) and remote patient monitoring (RPM) devices, such as healthcare wearables and medical equipment.

Additionally, digital ecosystems must support cloud services and third-party partnerships and application programming interfaces (APIs). They also need to comply with privacy and consent regulations, such as California Consumer Privacy Act (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA), in addition to facilitating secure data portability as mandated by the 21st Century Cures Act.

The challenges of meeting technical healthcare advancements with legacy IAM

In reality, healthcare organizations have to become digital enterprises in order to deliver a connected healthcare experience. Digital health ecosystems facilitate a continuum of care that drives preventative action. But while digital health ecosystems improve care, they also pose challenges.

Smart hospitals will deploy 7.4 million connected IoMT devices globally by 2026; over 3,850 devices per smart hospital.

– Juniper Research[5]

User access to both internal and external applications, systems, and services needs to be frictionless, yet incredibly secure. The management and privacy of customer data must be simultaneously made available and secure across a vast digital ecosystem consisting of multiple (and often disparate) systems and solutions. Additionally, users, IoT/IoMT devices, APIs, web apps, and services across all of those systems must also be seamlessly connected and secured.

For example, for patient care, providers must have immediate access to the customer data and history they need to inform their care regimen – and they must be able to share it securely with other associated providers and medical staff. This requires a single view of the customer based on data from multiple systems and accessible only to the relevant health team authorized by the customer. Lastly, all of the above must be done in a manner that provides a positive digital user experience.

Modern identity and access management (IAM) is the answer to all the challenges listed above. It is the technological backbone of digital health ecosystems.

Unfortunately, most healthcare IT consists of homegrown and legacy IAM solutions that weren't built to support today's digital health ecosystems spanning external-facing web, mobile, IoT/IoMT, and RPM sites. This lack in functionality has caused healthcare organizations to build and integrate homegrown and point solutions to fill the gaps, resulting in a complicated web of systems and data spanning on-premises and cloud environments. Homegrown and legacy IAM also make the connectivity and interoperability between systems and applications required by digital health ecosystems challenging. All of this results in less-than-ideal experiences that may drive customers, workforces, and partners away. On the other hand, a modern IAM platform can fully support today's digital health ecosystem requirements.

123%

increase in IoT malware attack volume in healthcare from 2020 to mid-2021[6]

A modern IAM platform, like the Ping Identity platform, helps organizations create dynamic and resilient digital health ecosystems for today and the future.

Using IAM to Surpass the Healthcare Interoperability Status Quo

To deliver the experiences, security, and interoperability required for profitability, healthcare organizations need an extensible identity platform purpose-built for consumer, workforce, B2B, B2B2X, and IoMT use-cases at any scale.

Ping Identity delivers all of this with a unified identity platform that helps healthcare leaders like you to modernize, integrate, and extend hybrid IT with full-suite, enterprise-grade identity and access management (IAM) and identity governance and administration (IGA) capabilities.

Ping Identity commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study to examine the potential return on investment (ROI) enterprises may realize by deploying Ping Identity CIAM.

133%
Customer conversion increase

400%
Increased engagement

$4.7M
Fraud impact over 3 years

40%
Reduction in security-related calls to the call center over 3 years

With Ping Identity customers improve customer experience and security, push out more releases and updates, and create net-new revenue streams. As a result, they see improved Net Promoter Scores℠, reduced login time, increased conversion rates, and improved customer lifetime value.

The following are five ways healthcare leaders can achieve similar results.

1. Modernize legacy IAM and integrate hybrid IT for interoperability

Despite technological advances, the expenses associated with maintaining and building out IT infrastructures means that most healthcare organizations are still saddled with legacy IAM systems. These systems lack transparency. They're fragmented, inflexible, and incapable of integrating hybrid IT environments and scaling to meet the needs of rapidly evolving digital ecosystems. And, they're incapable of supporting regulations such as the 21st Century Cures Act for data portability and interoperability. In short, legacy IAM systems are at odds with the digital world they need to accommodate. This limits healthcare innovation, new services, compliance, and the ability to respond quickly as digital health demands evolve.

96%

of healthcare executives say their organization's long-term success will depend on next-generation computing.

– Accenture[7]

Contrary to the above, modern IAM is purpose-built to tie legacy and modern infrastructures together. It eliminates identity fragmentation, replacing it with a single, unified approach. Modern, enterprise-grade IAM also supports data portability standards and is production-ready for hundreds of millions of users. Additionally, it supports collaborative identity partnerships that help healthcare organizations across industries realize their shared digital ecosystem vision.

With Ping Identity's identity capabilities, you can:

Modernize legacy IAM on your terms
Quickly and easily build on existing identity investments and streamline operations. Augment disparate legacy systems first and then coexist to later consolidate or retire solutions such as CA Single Sign-On (SiteMinder), Oracle, IBM, or homegrown systems.

Embrace hybrid IT
With a single IAM platform, run, unify, and secure all digital identities across hybrid IT and hybrid cloud. Eliminate identity silos and duplicate identities and data across mixed environments. Scale to support customers, workforce, partners, IoT devices, and services with the reassurance of a flexible, agile, unified platform architecture.

Manage multi-organizational identities by brand and theming
Flexibly organize identities by group (brands, partners, suppliers, agents, etc.) to enable advanced B2B2C scenarios at scale such as dynamic multi-brand experiences. Accelerate customer acquisition with truly immersive experiences tied to brand and channel preference. Lower operational costs with streamlined administration of complex multi-brand structures.

Support data portability for a shared ecosystem
Securely share data with third parties, with full support for standards such as OAuth, Fast Healthcare Interoperability Resources (FHIR), and user-managed access (UMA). Comply with Center for Medicare and Medicaid Services (CMS) mandates based on the 21st Century Cures Act.

Consolidate identities and connect everyone
Reduce IT costs and build on existing investments with a unified identity platform that works for customers, providers, workforces, partners, and IoT. Rapidly roll out new services to millions of customers and connected IoT/IoMT devices.

> **"Ping Identity is at the center of our business and our technology infrastructure. Without it, we'd have no way of securing, managing, and routing the millions of transactions occurring on our network every day."**

Jason Carmichael,
Manager of Enterprise Architecture, Availity

2. Enable personalized experiences that drive profitability

The easier it is to link identities and data and share them between stakeholders – like a provider and customer – the more able organizations are to deliver personalized experiences. By offering an exceptional, personalized experience for internal and external users, healthcare organizations can keep and attract customers and providers and grow their revenues.

93%

of healthcare executives report that their organization is innovating with an urgency and call to action this year.

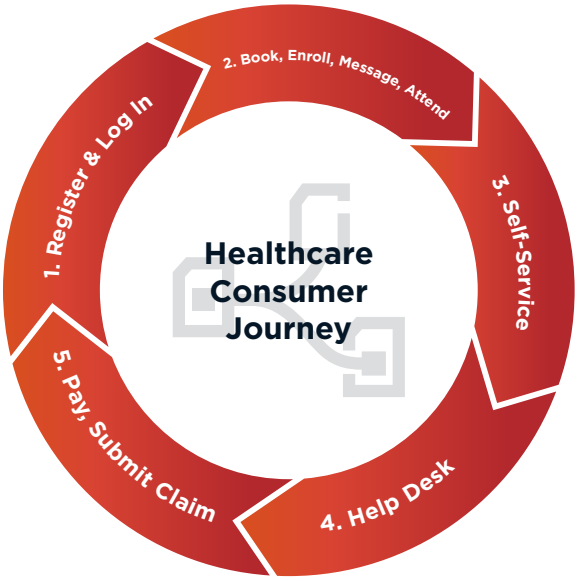
– Accenture[8]

Connected healthcare depends on providing a complete and consistent profile of each customer. This requires universally accessible, accurate, and up-to-date information, in addition to effective communication across digital channels. For example, care providers must have immediate access to patient data, including historical data, to inform their care regimen. They must also be able to share it securely with other associated providers and medical staff. In short, there must be a single view of the patient, accessible only to the relevant health team authorized by them.

Unfortunately, many healthcare organizations struggle with fragmented customer profiles. Information is manually aggregated and subject to human error. Siloed data makes it difficult to create a consolidated overview. Additionally, displaced or erroneous customer information delays care planning and compromises care quality. All of this results in frustrated customers and workforces.

> **"We want to make sure that our providers don't have to do tasks over and over again in order to do their job. I am confident that with Ping Identity we can simplify that process – like removing repetitive signing in and out throughout the day."**
>
> **Michael Kincaid,**
> Chief Information Officer, Partners Health Management

Ping Identity enables organizations with complete and consistent overviews of each customer, so they can tailor their experiences and care with ease. Ping Identity also allows healthcare organizations to consolidate the identity data of customers and the connected IoT/IoMT health equipment they are using. This means healthcare workers can treat every customer based on up-to-date data from multiple sources. This human-to-IoT relationship identity management makes data-driven, personalized treatments straightforward for providers and staff.



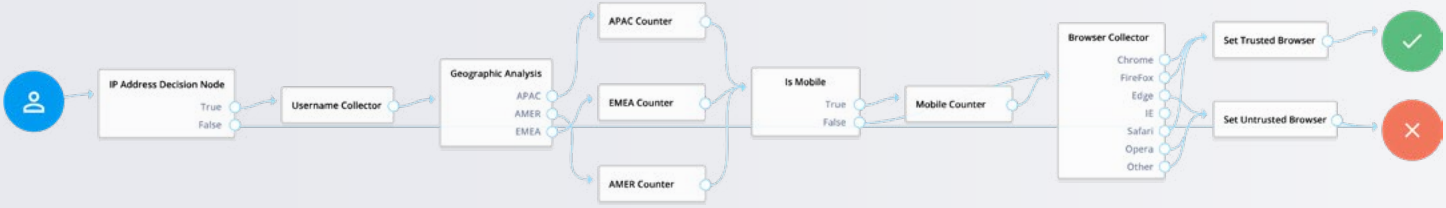
With Ping Identity, you can:

Leverage a Single, Organization-Wide View of the Customer

Integrate disparate systems to get a single view of each customer organization-wide for a unified customer profile across all digital channels. Share accurate, complete, and reliable data about customers with relevant parties during care planning and procedures.

Provide Custom User Journeys and Self-Service Options

Use a no-code, drag-and-drop interface to create customized registration and access journeys by user type. Enable users to self-serve password resets, account preferences, privacy settings, and data sharing.



Harness IoMT data sources

Collect data from disparate IoMT sources, such as wearables and remote patient monitoring (RPM) devices, and connect it to customer profiles to provide a holistic, real-time view of their health – even outside the traditional healthcare system.

Promote healthy living around the clock

Use real-time identity data to tailor services and care anywhere. For example, send real-time text alerts when a blood pressure monitor says a patient's blood pressure is too high, provide personalized payer plans based on health data from wearables, or enable customers to request medications at the click of a button.

3. Secure and integrate IoMT and map their relationships

Many healthcare organizations rely on an inefficient collection of incompatible systems to securely connect customers with devices and services. As the number of devices per customer grows – whether healthcare wearable, remote patient monitoring (RPM) devices, or smartphone with a payer's app – managing each device's identity and tying it back to the customer becomes more complicated and requires massive scale.

Healthcare organizations need to know that the internet of medical things (IoMT) devices they are deploying are secured, protected from breaches, and employing high-level authentication and authorization. Healthcare providers can modernize their services by building digital identity ecosystems that support new, user-friendly technologies that naturally evolve alongside the IoMT.

The Ping Identity platform was designed from the ground up for IoMT scale and complexity, so you can seamlessly connect customers, providers, and workforces to myriad devices, applications, and services.

The Ping Identity platform's flexible, scalable digital identity capabilities empower healthcare organizations to create seamless user experiences across channels by tying users, connected things, and cloud services to digital identities across digital health ecosystems. Within this ecosystem, Ping Identity's platform can register people, devices, and connected things, link them together, authorize and deauthorize their access to data, and apply policies that dictate security and privacy practices, as well as personalization.

With Ping Identity, you can:

Safely leverage and integrate IoMT identities and data

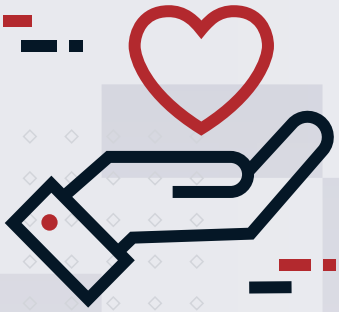
Secure and connect IoMT devices, systems, and data into customer services (such as member incentives) and care. Whether it's remote health monitoring tools keeping people safe and healthy, wearables, or apps, the ability to connect anything enables cohesive experiences, treatment, and beyond.

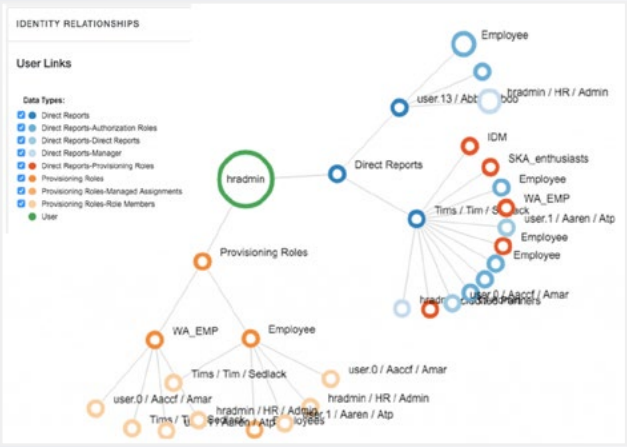
Manage the relationships between people, IoMT devices, and services

Manage the relationships between users, connected things, and application services. Secure registration and ensure device, user, and application authenticity, communication, sharing, and deregistration – all through a single identity platform.

Integrate and visualize data for informed care

Build graphs and dashboards that bring data to life and maximize its benefit by making it possible to analyze data pulled in across users, their devices, and services.





> **At Philips, we're on a mission to improve people's lives and to empower people to take better care of themselves and others. With the rise of cloud-based data, health and wellness apps, and customer sensors, it's important to be able to share all those sources of data with family members, health professionals, and others under close personal control.**

Jereon Tas,
CEO Healthcare Informatics Solutions and Services, Philips

4. Deliver continuous, intelligent security and prevent fraud

According to the Ping Identity Consumer Breach Report, for the fourth year in a row, healthcare was the biggest target in terms of the number of breaches, accounting for 24% of the total. It was also the most costly at $614 per record. Web application attacks[9] and unauthorized access are the main causes for breaches.[10] Reports also show that 90% of the 10 largest healthcare data breaches in 2022 were linked to third party-vendors.[11]

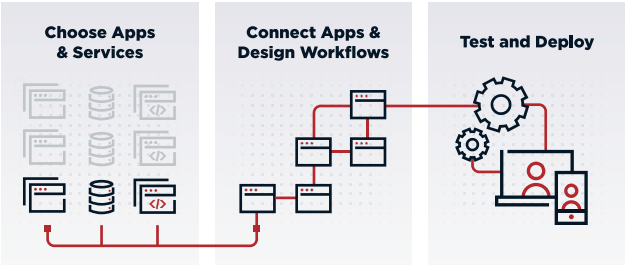
> **Security is now part of the business. This is the new reality. Our customer ID management is in the middle of everything the business does and it's very important for the business's success. We're not just there to support the business, we are part of the business.**
>
> **Eliran Hayun,**
> Principal Cybersecurity Architect, HCSC

Healthcare leaders are under constant and significant pressure to keep sensitive customer data and connected devices secure. It is no longer enough to simply authenticate and authorize access "at the door." Now, activity must be monitored throughout an online session for suspicious behavior or unusual activity that might be malicious.

Any compromise in security can lead to a breach and potentially irreparable consequences. The authenticity of digital relationships must be constantly verified, and organizations must be able to revoke access or deny requests if necessary.

Common questions healthcare IT leaders ask are:

- How do I ensure security without disrupting other critical processes?
- How do I confirm the authenticity of your customers and/or caregivers as they move through the health ecosystem?
- How do I assess if an authentication attempt or any behavior post-authentication might be fraudulent?
- Can I track customers, workforces, and partners through their authentication journey, and flag them for additional authentication as their behavior changes?



Ping Identity offers full support for advanced security models, such as Zero Trust and Continuous Adaptive Risk and Trust Assessment (CARTA), with industry-leading artificial intelligence (AI) and machine learning (ML) features and third-party integrations, so healthcare organizations can meet the sophistication of cybercriminals at scale. This includes the ability to add customer and IoMT context to authentication so that organizations can continuously authorize every transaction across their enterprise. Additionally, with Ping Identity, organizations can centralize identities across their hybrid IT architecture to improve audits and compliance with full user lifecycle management.

With Ping Identity, you can:

Protect consumers and your organization

Integrate with legacy systems and environments to apply Zero Trust organization-wide. Secure hybrid IT environments – from legacy on-premises networks to modern mobile apps, APIs, microservices, and more. Leverage intelligent, contextual, continuous security to protect customers, workforces, devices, and IoMT at scale.

Provide frictionless security

Use a no-code interface to build, customize, and adjust access journeys. Apply adaptive access using identity and non-identity context for the right amount of friction. Adjust friction according to risk. Trust but verify at all times using device and environmental context during authentication attempts to ensure devices are trusted.

Layer AI and ML on top of existing investments

Use AI, ML, and advanced pattern recognition to prevent cyberattacks and detect fraud in real time while enabling smarter access decisions to enhance the experience of legitimate users.

Solve access challenges caused by siloed environments by layering AI and ML on top of existing identity governance and administration (IGA) solutions. Collect and analyze identity data such as accounts, roles, and entitlements to identify security access and risk blind spots.

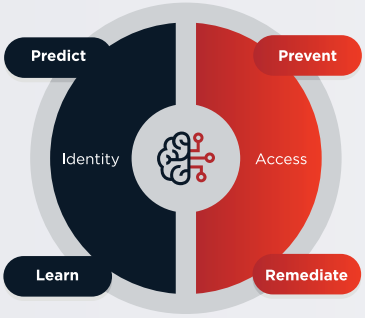
Engage both sides of identity brain simultaneously to give the right access to the right people (or things) at the right time

Autonomous Identity

Reduce cost and minimize risk

Understand & Automate

Use AI/ML to understand who or what should have access with enough confidence to automatically approve, provision and certify



PingOne Protect

Delight and protect users

Continuously Protect

Use AI/ML to continuously inspect and adapt real-time access based on behavior; orchestrate real-time response and remediation

Detect and mitigate fraud

Detect and prevent fraudulent transactions through advanced capabilities and fraud technology. Continuously collect and interpret multiple signals about a user–their device, network, reputation, and known behaviors– and then makes fine-grained access and authorization decisions for any high-stakes transaction.

Delegate the administration of access to third-parties

Use delegated administration to distribute the responsibility of managing user access across different roles or departments. This approach ensures that the right individuals have appropriate access to critical systems and information while maintaining data confidentiality, integrity, and security. It also enables the ability to scale go-to-market initiatives by delegating control to business partners to manage downstream access, such as with B2B2C scenarios.

5. Keep sensitive data private and address regulations

Customer confidentiality is paramount in healthcare. Keeping personal data secure is not just about regulatory compliance, it's also about building trust and protecting customer relationships. Organizations must ensure that the identities of users, connected things, and cloud services are verified and authorized. Healthcare organizations must secure sensitive health data and share it with relevant people, third-parties, and devices that depend on it to provide optimal services and care.

There are a number of key factors to consider in managing data privacy and compliance. For example:

- How do customers consent to share data with your organization?
- What services, devices, and third-party partners do they use?
- How easy is it to scale this permission management as the user base grows?
- How do you audit the sharing of customer data?

Ping Identity protects customer privacy and helps address data protection regulations.

> **Ping Identity has really helped us with how we manage users' profiles and consent. Doing that seamlessly, even when moving customers between channels or between our properties and partners, is a game changer.**
>
> **John Tryon,**
> Head of Information Security, HCSC

User-Managed Access (UMA) enables healthcare organizations to give customers control over their health data. Customers can determine who gets access to their data, for how long, and under what conditions. They can authorize data sharing with the appropriate providers and care providers and encourage greater collaboration between all stakeholders involved in their healthcare experience.

Ping Identity simplifies complex data sharing and consent activities by enabling customer controlled data sharing across cloud, mobile, and IoT sources.

With Ping Identity, you can:

Enhance consumer trust and mitigate risk
Scale permissions management to tens of millions of customers. With a user-friendly privacy and consent dashboard, give customers fine-grained control to manage their own profile details, the devices and data from things like wearables that are connected to their account, applications they have consented to connect to their account, and how they choose to share data – such as with third-party providers and family members.

Meet regulatory mandates
Address regulations such as Joint Commissions, HIPAA, NIST 800-63, HITECH, CCPA, and the CMS Interoperability Mandate. Securely share data with third parties, with full support for standards such as OAuth, Fast Healthcare Interoperability Resources (FHIR), OpenID Connect (OIDC), and user managed access (UMA). Use a "share button" to initiate simple, standardized mechanisms for authorization and API security across all relevant healthcare services according to needs.

Why healthcare leaders choose Ping Identity

Ping Identity is the leading enterprise-grade IAM provider, helping people simply and safely access the connected world. Top healthcare organizations use Ping Identity to modernize and accelerate digital transformation, support their digital healthcare initiatives, and secure their users and the organization.

FORRESTER®

LEADER
Forrester Wave™ Customer Identity and Access Management, Q4 2022

Gartner®

LEADER
Magic Quadrant Leader for Access Management 2022

kuppingercole ANALYSTS

OVERALL LEADER
KuppingerCole Leadership Compass, CIAM Platforms, 2022

Consume as-a-Service or deploy in any cloud

Enjoy fast, efficient deployments with the reliability needed for critical use cases and a responsive vendor on hand. Learn more about Ping Identity deployment options.

Learn more about how Ping Identity can help your organization

Digital health ecosystems require a flexible, comprehensive IAM platform. Contact us to learn how Ping Identity can help you achieve your digital healthcare goals.

Ping Identity helped a North American healthcare payer with over 20 million members strategize and implement their customer identity and access management (CIAM) initiative. With Ping Identity, the company increased member satisfaction and registrations, reduced risk by securing member identity credentials, established a stable environment that can scale, and obtained readiness for their Center for Medicare and Medicaid Services (CMS) interoperability requirements.

[1] https://www.grandviewresearch.com/industry-analysis/digital-health-market

[2] https://healthcaretransformers.com/healthcare-business/strategy-and-operations/top-10-healthcare-trends-for-2023/

[3] https://www.ama-assn.org/press-center/press-releases/ama-physicians-propelling-health-care-s-digital-transformation

[4] https://www.pwc.com/us/en/industries/health-industries/library/behind-the-numbers.html

[5] https://www.juniperresearch.com/press/smart-hospitals-to-deploy-over-7mn-iomt

[6] https://healthitsecurity.com/news/iot-malware-attack-volume-up-123-in-healthcare

[7] https://www.accenture.com/us-en/insights/health/digital-health-technology-vision?c=acn_glb_digitalandintelbusinesswire_13142618&n=mrl_0622

[8] https://www.accenture.com/us-en/insights/health/accenture-digital-health-technology-vision-2021

[9] https://www.verizon.com/business/resources/reports/dbir/2022/healthcare-data-breaches/

[10] https://www.forgerock.com/resources/analyst-report/2022-forgerock-consumer-identity-breach-report

[11] https://www.hhs.gov/sites/default/files/2023april6-emrs-top-target-cyber-threat-actors.pdf