



IMPROVE AND SECURE HEALTHCARE DELIVERY WITH DIGITAL IDENTITY



WHITE PAPER

TABLE OF CONTENTS

03

04

INTUITIVE JOURNEYS
SEAMLESS ENGAGEMENT
ONLINE HEALTH PRIVACY

08

RAPID ONBOARDING & INTEGRATION
ZERO DOWNTIME RATIONALIZATION

11

HIPAA & HITECH COMPLIANCE
COMPREHENSIVE ACCESS SECURITY
 Challenge
 Ping Solution

14



INTRODUCTION

The consumerization of healthcare is driving a cascading force of differentiation from payers to providers to pharmaceutical and life sciences organizations. This shift, combined with value-based payments, underlies your charge to improve patient and member outcomes and experiences with new services, M&A and unprecedented cross-industry partnerships.

“Only 48% of U.S. adults 18 or older have insurance provided through their employer. The remaining population is getting their insurance elsewhere in ways that require more consumer choice.”¹

Consumers have more healthcare choices than ever, meaning payers and providers have more competition as well. Many are differentiating themselves in the marketplace by adding health tracking apps and integrating with partners to display prescription, billing and appointment information.

To further differentiate, payers and providers are acquiring their regional and cross-industry counterparts to lower costs and improve leverage in purchasing and reimbursement decisions. Meanwhile, pharmaceutical and life sciences organizations are seeking to improve outcomes, interacting directly with patients by developing medication adherence applications.

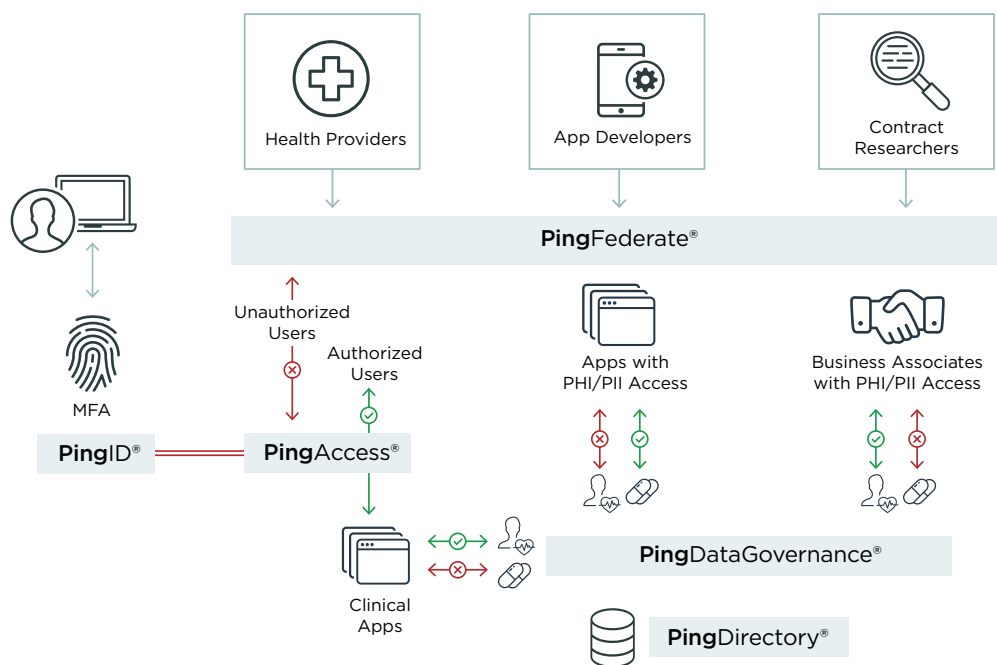
Successfully differentiating through these means isn't easy. And it requires prioritizing seemingly opposing initiatives. On the one hand, you must deliver improved patient and member experiences. On the other, you must give equal focus to privacy and security measures.

Your patients and members are also today's consumers, and they expect seamless user experiences. But you can't meet their demands at the expense of security. You must remain a stalwart steward of protected health information (PHI) and personally identifiable information (PII). The distributed nature of healthcare delivery and R&D make this an especially difficult balancing act.

Read on to learn how the Ping Identity Platform creates a solid identity and access management (IAM) foundation and helps hundreds of healthcare payers, providers and life sciences organizations like yours achieve better experiences and outcomes.

THE PING IDENTITY PLATFORM

Figure 1: How the Ping Identity Platform addresses the challenges of today's healthcare organizations.



Rebecca McAdams and Carlton A. Doty, "Health Insurers: Prepare for Survival of the Fittest," Forrester Research, Sept 2 2015.

IMPROVE PATIENT AND MEMBER EXPERIENCES

Your patients and members want to engage with you when and where it's most convenient for them. Just like their favorite product and service providers, you're expected to provide online portals and mobile applications. They want you to provide intuitive ways to register, engage with personalized health information and complete tasks like scheduling and billing. Rounding out their list of requirements, your patients and members also expect virtual care delivery, digital health tracking and online health diaries.

Wherever you are on your "improving patient and member experience" journey, a robust, flexible IAM solution is a firm foundation on which to introduce and scale these experiences.

INTUITIVE JOURNEYS

Healthcare organizations often interact with diverse and sometimes distinct populations through their online portals. Patients and members of different age groups and backgrounds, along with providers, billers, brokers and researchers, all utilize health portals for a variety of reasons.

Many healthcare organizations struggle with providing intuitive online journeys for these disparate populations. This is often a function of the limited options available from their current identity and access management solutions. These legacy and often homegrown solutions weren't designed for today's demands.

The Ping Identity Platform can help you deliver the intuitive journeys your patients and members expect. It offers a range of registration, authentication and self-service options that you can customize to serve the needs of each user population. Figure 2 provides an overview of the options that can be delivered by the Ping Identity Platform, while Figure 3 illustrates how you might address members versus providers.

MIX & MATCH

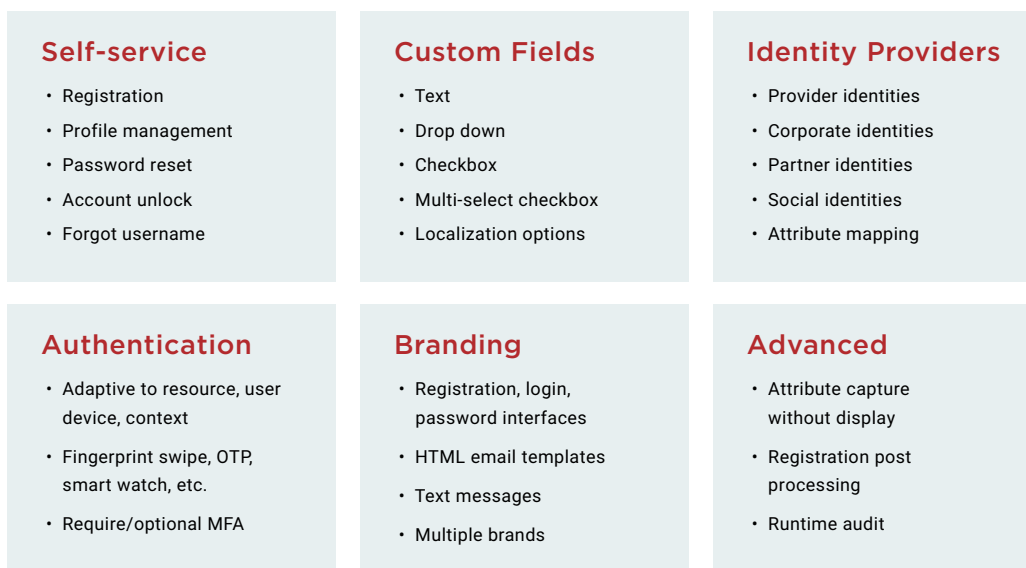


Figure 2: The Ping Identity Platform provides mix-and-match capabilities to meet the needs of diverse user populations.





	MEMBERS	PROVIDERS
Self-service	Enable all self-service options to provide maximum flexibility	Limit self-service options to preserve integrity of online prescription approval
Custom Fields	Capture social security numbers	Capture medical license numbers
Identity Providers	Require online registration	Support the use of hospital/clinical credentials
Authentication	Offer optional MFA to access health profiles	Require multi-factor authentication to approve prescription orders
Branding	Custom to the plan purchased by the member	Custom to the specialty of the healthcare provider
Advanced	Upon date of birth entry, record date of birth and member age in the directory	When certain hospitals are entered, require entry of the specific unit of care

Figure 3: Examples of how you might structure capabilities to meet the requirements of members vs. providers

SEAMLESS ENGAGEMENT

Healthcare organizations aren't immune to the customer experience (or CX) trend that's dominating the traditional business world. The importance of CX is seen in the transformation of health portals, which were once little more than digital portfolios of information, into full-on customer engagement centers. What formerly were places to view bills and lab results are now avenues to chat with your doctor and track health metrics in real time.

Evolving your enterprise from predominantly providing information access to delivering true patient and member engagement is anything but easy. For starters, you don't just have your own resources to manage, but you must also address dozens—maybe even hundreds—of third-party apps and APIs. To further complicate matters, your patient and member data can become increasingly scattered and disjointed as your channels of health engagement multiply. And on top of all of this, you must provide patients the ability to manage consent for every resource and person with access to their data.

The Ping Identity Platform makes these seemingly daunting challenges much simpler to solve.

Provide Single Sign-on for All Users and Resources

To give your patients and members single sign-on (SSO) to your expanding portfolio of health apps, APIs and third-party resources, you need a robust set of identity federation capabilities. The Ping Identity Platform, specifically PingFederate, provides the flexibility to connect any identity to any application or API with federation hub capabilities. You're able to connect diverse populations of patients, members, providers, brokers and researchers to any application they require. And with built-in support for identity standards like SAML, WS-Fed, WS-Trust, OAuth and OpenID Connect, you're ensured of the interconnectivity you need with third parties.

Unify Health Profiles with Centralized Sharing Options

Imagine a patient or member takes a health assessment one week, chats with a wellness coach the next week and receives virtual care shortly after that. Now, imagine how easy (or difficult) your current platform makes it for this same person to retrace their steps and find important information about these activities a few months later.

PingDirectory, Ping Identity's secure directory, can synchronize data from select applications to personalize patient and member experiences. Its flexible schema accommodates unique health attributes to present a unified health profile.

Once a unified patient profile is assembled, PingDataGovernance enables user-friendly data sharing with health proxies. After capturing consent, PingDataGovernance can also enable and enforce policies around the sharing, viewing and managing of health profile data by certain providers and dependents.

ONLINE HEALTH PORTAL

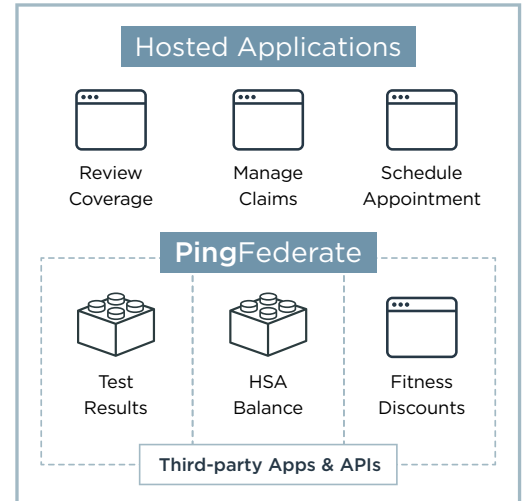


Figure 4: PingFederate provides the flexibility to connect any identity to any application or API.

PingDirectory®

PingDataGovernance®

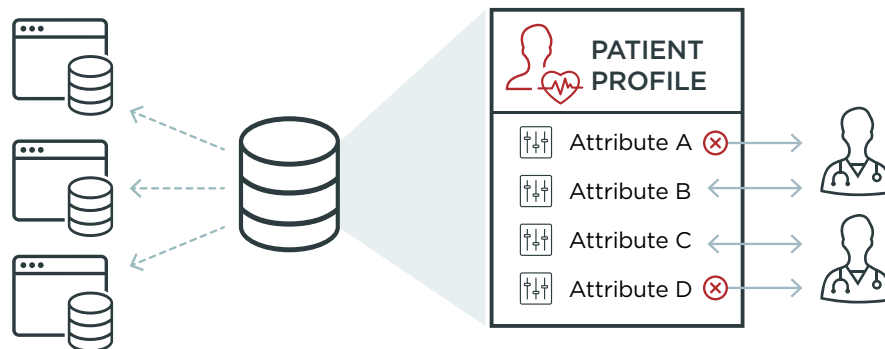


Figure 5: How PingDirectory and PingDataGovernance work together to enable a unified profile and enforce policies.

ONLINE HEALTH PRIVACY

You already understand that patient and member data needs to be secure. But privacy is another aspect of security that deserves a closer look. Because of the personal nature of information shared with healthcare providers, your users might be wary of using your digital properties. In a world where one's personal online activities are sometimes made public, your patients and members may fear that inadvertently leaving a browser open or a phone unlocked could reveal confidential information to a friend or family member, or worse yet, someone with ill intent.

PingID, the Ping Identity Platform's cloud-delivered MFA solution, can be offered as an optional measure for patients to enable another layer of security to access their online health profiles. Additionally, the PingID mobile SDK can be embedded in mobile apps to provide an extra layer of privacy by requiring an additional authentication to view sensitive health and profile data, like prescription notifications.

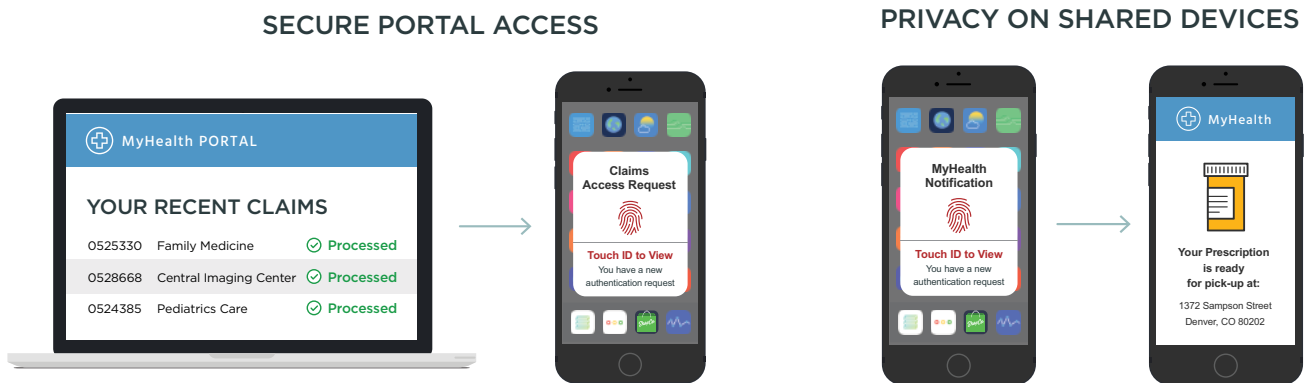


Figure 6: The PingID mobile SDK can provide additional security by requiring additional authentication to access sensitive data.

You may think that an improvement in security and privacy must naturally result in a diminished user experience. While this once held true, you no longer need to sacrifice experience to optimize security. Using adaptive authentication, PingID can be customized to step up authentication for higher-risk transactions only, such as editing or deleting PHI. Supporting popular user-friendly mobile push notification options—including swipe to authenticate, fingerprint and Face ID—PingID can be customized to notify users of the changes being requested before they're made.

PingID also enables patients and members to self-manage a network of trusted devices approved for access to their health data. When an unrecognized device is used for access, PingID can require an additional authentication before granting access. These flexible authentication methods support a wide range of use cases, enabling you to improve user experiences for your patients and members, while maintaining their privacy and security.

SUPPORT INTEGRATED HEALTHCARE DELIVERY

Population health management, value-based care and increasing price sensitivity are driving unseen levels of integrated healthcare delivery. Mergers and acquisitions are quickly becoming the norm, with consolidation occurring more frequently and faster than ever before.

Innovative partnerships are also on the rise, as healthcare payers and providers form joint ventures to coordinate care and manage population health. Similarly, pharmaceutical organizations are partnering with universities, hospital systems and contract research firms to accelerate the introduction of new drugs.

Integrated healthcare delivery promises economies of scale, improved outcomes, portfolio diversification and faster time to market. But these benefits also present new challenges. To reap the rewards, you need a solution that can accelerate integration of new acquisitions and partners without disrupting your business. The Ping Identity Platform provides this solution.

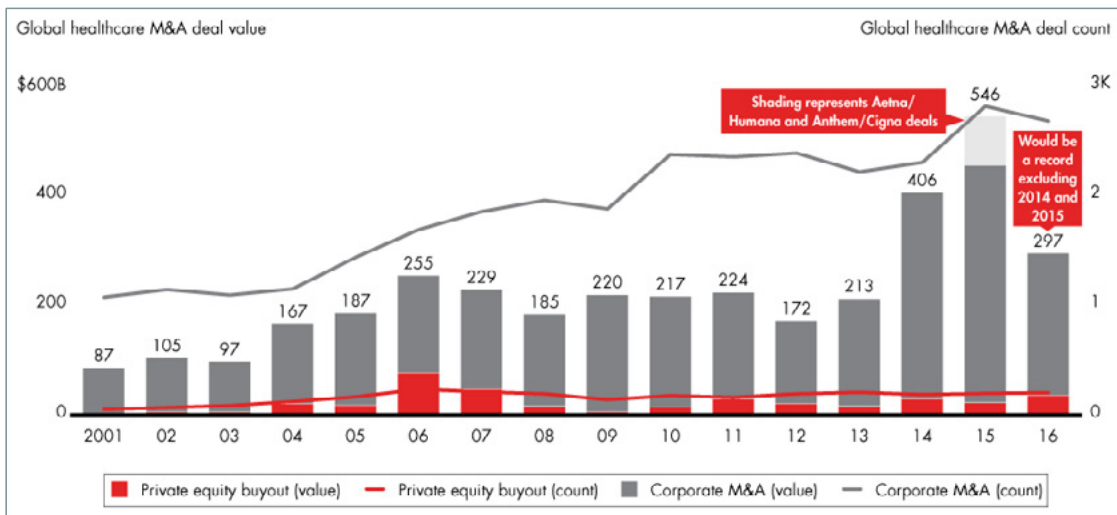


Figure 7: Healthcare M&A activity rose sharply starting in 2014, with 2015's total deal value of \$546B more than doubling the previous high of \$255B in 2006.²

² Kara Murphy, Nirad Jain, Joshua Weisbrod, Franz-Robert Klingan, Vikram Kapur, Justin Doshi and Jeff Haxer, "Global Healthcare Private Equity and Corporate M&A Report 2017," Bain & Company, Apr 19 2017.



RAPID ONBOARDING & INTEGRATION

New partnerships, mergers and acquisitions are often formed with projected timelines of when the joint entity will be fully operational. Often, these projections fail to capture the difficulty of providing access to diverse resources. Providing only a surface-level view, they don't adequately account for the complexity of managing and securing access to multiple domains for a variety of roles.

You'll find support for your identity and access management integration challenges in the Ping Identity Platform.

Federation Hub: PingFederate and PingOne connect any identity to any application or API with federation hub capabilities. Your employees can connect to any acquired or partner application, or API, in any domain, and vice versa.

Hundreds of SaaS Integrations: Combine federation hub capabilities with out-of-the-box connectors to Office 365, Salesforce, Dropbox, ServiceNow and others to immediately connect your newly acquired identities to resources.

Dozens of Enterprise Integrations: Federation hub capabilities also enable out-of-the-box connectors to apps from Oracle Weblogic, IBM Websphere, Sharepoint.

PingAccess for AzureAD: Whether the acquiring or the acquired organization is using AzureAD to manage identities, PingAccess can be deployed to provide centrally managed access control to all on-premises applications at either organization.

AWS Deployment Automation: Deploy centrally managed access control to an acquired entity's AWS instance in minutes with pre-integrated reference architectures. You can take advantage of AWS auto-scaling for apps with unfamiliar demand patterns and customize access security in the most efficient manner for each resource.

Accenture MSP: If integration resources are temporarily tied up, or your long-term strategy is to utilize a managed service provider for identity and access management, Ping has partnered with Accenture's Velocity Identity Program to provide high-scale, enterprise-grade identity services.

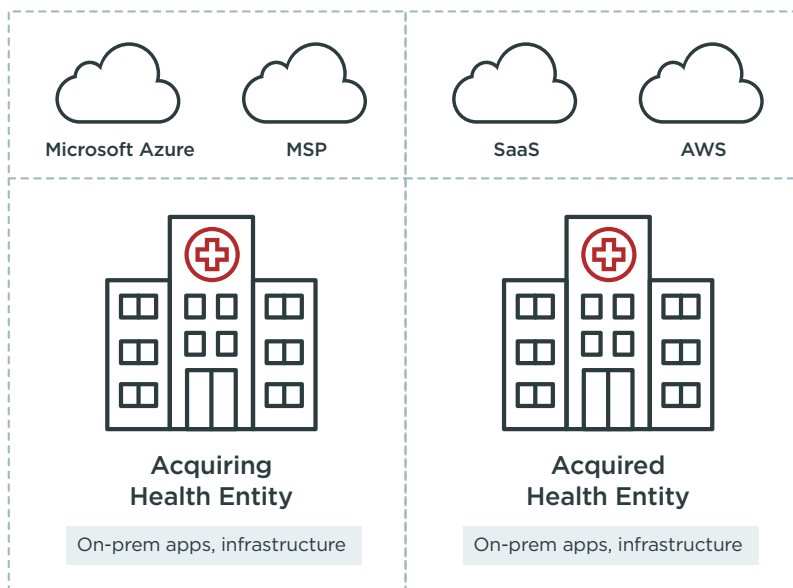


Figure 8: The Ping Identity Platform facilitates integration through out-of-the-box connectors with popular cloud-based services.

ZERO DOWNTIME RATIONALIZATION

The potential economies of scale when healthcare entities combine can be significant. But payers, providers and pharmaceutical organizations are often cautious about rationalizing systems too quickly (or at all) for fear of disrupting business as usual.

Today, many healthcare organizations run multiple homegrown and legacy IAM systems for different groups of applications and those who use them. The hardware, licensing, administrative and productivity costs of this approach have magnified as the winds of M&A have swept across healthcare. To ensure smooth integration, the Ping Identity Platform is designed to help you maintain secure access to critical resources during IAM rationalization.

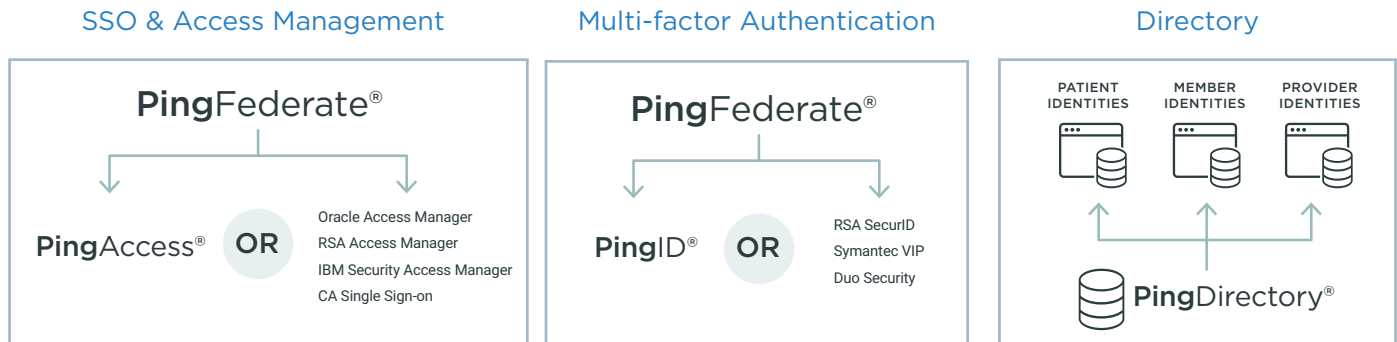


Figure 9: The capabilities of the Ping Identity Platform support IAM rationalization efforts, while ensuring uninterrupted access to critical resources.

Single Sign-on & Access Management

Patients, members and providers require uninterrupted access to critical health resources. Ping offers WAM integration kits and token translators to accelerate migration from legacy SSO and WAM providers. Best practice migration guides are also available to support your zero downtime transition from CA Siteminder (SSO), RSA Access Manager and Oracle Access Manager.

Multi-factor Authentication (MFA)

You can't afford downtime and resulting "security exceptions" when rationalizing MFA-protected resources, particularly those containing e-PHI. Ping provides integration kits and adapters for legacy MFA solutions, including RSA SecurID and Symantec VIP, for a zero downtime rationalization or planned period of coexistence with cloud-based MFA solutions, like PingID.

Directory

Critical health apps rely on directories to authenticate users. So when directories go down, members, patients and providers lose access. PingDirectory can replace multiple directories without downtime through bidirectional data synchronization. You're assured information is up to date before you take steps to deprecate legacy identity stores. PingDirectory is also equipped with a client SDK to mimic proprietary behaviors that apps may expect from the original directory.

MAINTAIN COMPLIANCE AND PREVENT BREACHES

When it comes to the level of effort required to remediate a data breach, there's no industry quite like healthcare. The very initiatives intended to improve patient and member experiences have also expanded the breach attack surfaces, as hundreds of new apps now handle sensitive PHI and PII.

Integrated healthcare delivery requires sharing the same data with more non-employee health partners than ever before. These trends greatly expand the scope of root cause investigations, victim identification efforts and many other breach remediation activities. They've also attributed to healthcare having a per capita data breach cost substantially higher than other industries.³

Improved patient and member experiences—and outcomes—are on the horizon. And they don't have to come at the cost of data breaches and compliance violations. A comprehensive IAM strategy can help you maintain HIPAA/HITECH compliance. Beyond compliance, it can help you prevent breaches of electronic PHI from compromised credentials and deficient access security measures.

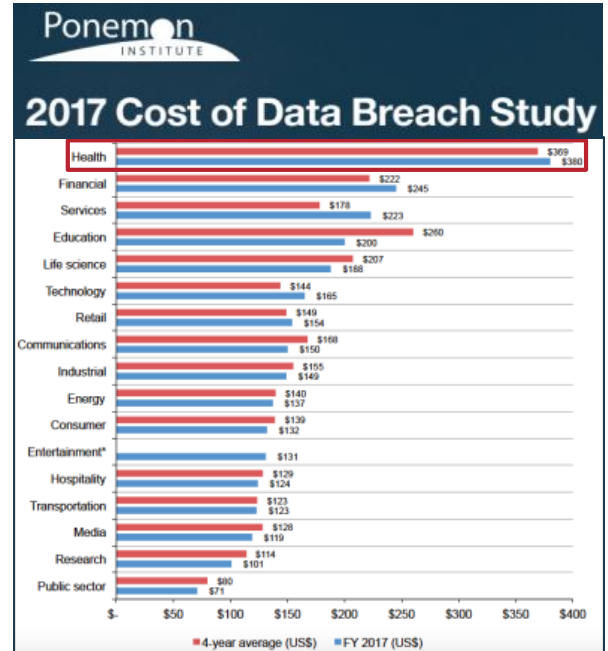


Figure 10: The per capita cost of a data breach in healthcare far exceeds that of other industries.⁴

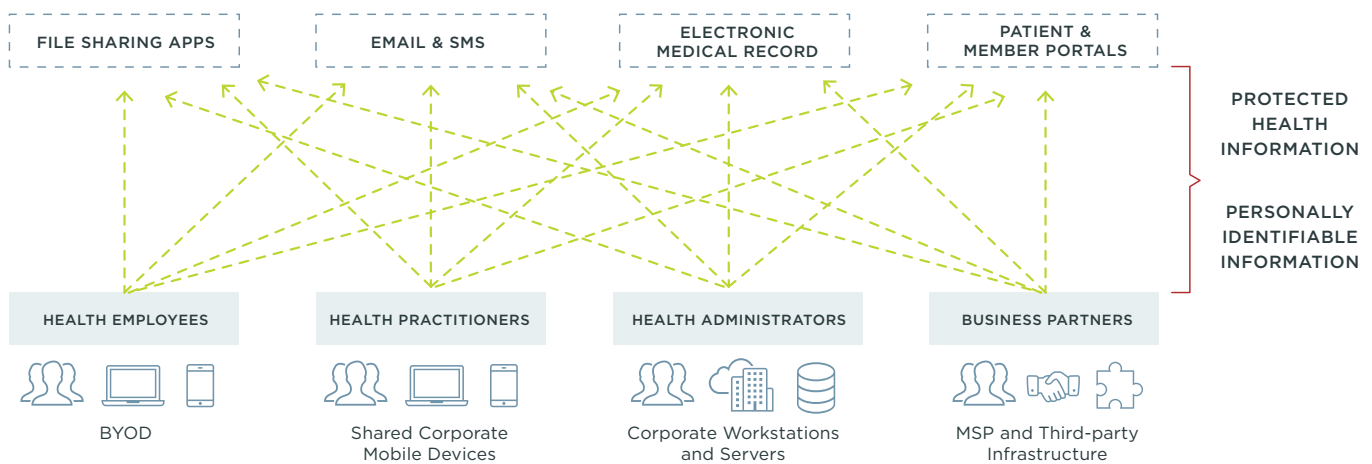


Figure 11: More people, devices and resources are handling PHI and PII, contributing to an increased attack surface and the subsequent high cost of healthcare data breaches.

³ Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview

⁴ Ibid

HIPAA & HITECH COMPLIANCE

In the HIPAA Security Rule, the Department of Health and Human Services (HHS) provides implementation guidance around setting up “minimum necessary” access controls to prevent inappropriate usage of e-PHI. It recommends specific administrative, physical and technical safeguards to ensure the integrity of health data.

“A lack of access controls and regular review of audit logs helps hackers or malevolent insiders to cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen.”

Robinsue Frohboese | Acting Director, HHS Office for Civil Rights

These recommendations guide healthcare organizations toward a comprehensive access control framework. Yet, the two largest fines issued for HIPAA violations in the history of the regulation—one for \$5.55 million and the other for \$5.5 million—were both the result of insufficient security.

The Ping Identity Platform can help you bridge the chasm between recommendation and implementation. Offering support for a number of administrative and technical precautions as illustrated in Figure 12, the Ping Identity Platform can help you comply with HIPAA and avoid costly fines.







<p>45 C.F.R. § 164.308(a)(4)(i) Policies and procedures for authorizing access to e-PHI only when such access is appropriate</p>		<p>PingFederate, PingID, PingAccess & PingDataGovernance use identity attributes to determine appropriate, minimum necessary access to e-PHI & PII during authentication, at the URL level and the data layer of applications</p>
<p>45 C.F.R. §§ 164.310(b) & (c) Policies and procedures to specify proper use of and access to workstations and electronic media</p>		<p>PingID can be used as primary authentication to secure workstations and electronic media</p>
<p>45 C.F.R. § 164.312(a) Policies and procedures that allow only authorized persons to access electronic protected health information</p>		<p>PingFederate, PingID, PingAccess & PingDataGovernance use behavioral, browser and network policies to determine appropriate, minimum necessary access to e-PHI and PII during authentication, at the URL level and the data layer of applications</p>
<p>45 C.F.R. § 164.312(b) Mechanisms to record and examine access and other activity in information systems that contain or use e-PHI</p>		<p>PingAccess & PingDirectory log and audit access and transactions within apps and identity stores containing e-PHI</p>
<p>45 C.F.R. § 164.312(c) Policies and procedures to ensure that e-PHI is not improperly altered or destroyed</p>		<p>PingAccess ensures e-PHI isn't improperly altered or destroyed by limiting transactions according to user/device attributes and context</p>
<p>45 C.F.R. § 164.312(e) Guard against unauthorized access to e-PHI that is being transmitted over an electronic network</p>		<p>PingDirectory encrypts e-PHI transmitted over electronic networks</p>

Figure 12: How the Ping Identity Platform's capabilities map to specific HIPAA compliance safeguards.

For a more complete overview of how the Ping Identity Platform supports HIPAA compliance and addresses the concerns of the healthcare CISO, CIO and CMIO, read the whitepaper: [Seamless and Secure Healthcare Delivery with the Ping Identity Platform](#).

COMPREHENSIVE ACCESS SECURITY

As a healthcare organization, you already know that achieving HIPAA compliance is only the first step in building a comprehensive access security framework. In fact, HIPAA purposely avoids prescribing specific technologies with an understanding that compliance is usually part of a larger defensive strategy. But building a strong framework becomes more challenging as the scope of resources and identity types under consideration expands and becomes more diverse.

As shown in Figure 13, the Ping Identity Platform provides solutions to address many of the challenges healthcare organizations face today.

CHALLENGE	PING SOLUTION
<p>Credential Reuse An ever-expanding portfolio of patient, member, clinical and research applications means the reuse of usernames and passwords will continue to proliferate.</p>	<p>Single Sign-on for all Applications Minimize credential reuse and provide seamless access by enabling SSO to your in-house and third-party applications.</p>
<p>Insecure Smart Cards Some healthcare IAM vendors choose convenience over security, using convenient, but insecure password replay methods over smart cards.</p>	<p>Secure Identity Federation Replace insecure password replay with easily integrated and more secure identity federation methods, while maintaining the use of smart cards.</p>
<p>Authentication without Context Integrated healthcare delivery means you need to give third parties access to sensitive health data, but you still must protect that data.</p>	<p>Adaptive Authentication Enable step up authentication during high-risk transactions and when access is requested from unrecognized devices and IP addresses.</p>
<p>Decentralized Data Governance Growing your portfolio of patient and member experience apps requires giving developers access to more health data and risking non-compliance with regulations.</p>	<p>Centrally Governed Access to Data Centralize governance of access to certain types of data, and ensure that app developers comply with recommended precautions.</p>
<p>Decentralized Access Policies The organizations that you partner with or acquire may have security postures that don't match your own and could put you at risk of regulatory violation and breach.</p>	<p>Centralized Access Security Policies Ensure partners comply with suggested safeguards by centralizing enforcement of data sharing, viewing and management policies.</p>

Figure 13: The Ping Identity Platform solves for some of the biggest challenges facing healthcare organizations today.



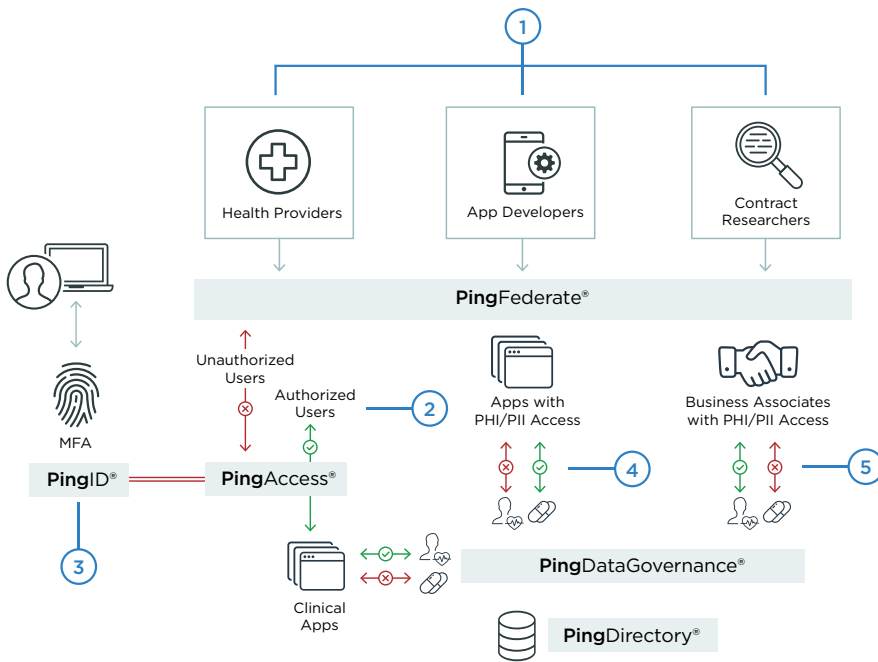


Figure 14: How healthcare organizations are using the capabilities of the Ping Identity Platform to deliver improved experiences and strengthen security and privacy.

- 1 **Provide Single Sign-on**
Reduce credential reuse by providers, patients, members, health and business partners
- 2 **Replace Insecure Smart Cards**
Protect critical health apps by replacing insecure smart card password replay technologies with secure identity federation with out-of-the-box smart card integrations
- 3 **Implement Adaptive Authentication**
Step up authentication with user and device context to provide secure and seamless access for all providers and business partners
- 4 **Centrally Govern Access to PHI/PII**
Ensure app developers comply with HIPAA and HITECH by centrally managing access to data
- 5 **Centralize Access Policies**
Ensure business associates comply with HIPAA/ HITECH by controlling access to all applications and APIs in one place

CONCLUSION

Rising costs are fueling a massive transformation in how health services are sought out and delivered around the globe. In this new era of healthcare, improved patient and member experiences are a must. And integrated healthcare delivery provides the promise of improved outcomes.

Those healthcare providers, payers and pharmaceutical organizations who can adapt quickly and securely, without disrupting their businesses, will emerge as the leaders.

The Ping Identity Platform is a healthcare IAM solution that enables you to give the right people access to the right things. From physicians to patients to third parties, all of your users can enjoy easy access to your growing portfolio of applications and APIs. And you can rest assured you're not compromising data security or compliance.

Relied upon by hundreds of healthcare payers, providers and life sciences organizations, the Ping Identity Platform helps you:

- Improve patient and member experiences.
- Support integrated healthcare delivery.
- Prevent data breaches and maintain compliance.

To learn more about how the Ping Identity Platform can improve your patient and member experiences, and your own business outcomes, visit www.pingidentity.com/healthcare.

Ping Identity envisions a digital world powered by identity. As the identity security company, we simplify how the world's largest organizations prevent security breaches, increase employee and partner productivity and provide personalized customer experiences. Enterprises choose Ping for our identity expertise, open standards leadership, partnership with companies like Microsoft, Amazon and Google, and collaboration with customers like Boeing, Cisco, GE, Kraft Foods, Walgreens and over half of the Fortune 100. The Ping Identity Platform allows enterprises and their users to securely access cloud, mobile and on-premises applications while managing identity and profile data at scale. Architects and developers have flexible options to enhance and extend their existing applications and environments with multi-factor authentication, single sign-on, access management, directory and data governance capabilities. Visit pingidentity.com.