Seamless and Secure Healthcare Delivery with the Ping Identity Platform

Written By: Drew Labbo

MBA, CISSP

Contents

Introduction

Healthcare is one of the most heavily regulated industries in the United States and the world. Healthcare provider organizations, laboratories, payers, healthcare clearinghouses, and business associates—such as pharmaceutical companies, medical device manufacturers, and software companies—are challenged to contain the cost of healthcare, comply with multiple regulations, and enable a high standard of patient care. The Ping Identity Platform offers broad integration points with clinical and business operations and workflow, improving productivity and security with identity and access management (IAM) solutions.

Healthcare Providers

Boards of directors and management teams at healthcare provider organizations are challenged to provide higher quality patient care for lower cost, all while aligning with a modern healthcare model that is shifting toward capitated compensation for keeping patients healthy rather than fee for healthcare services. These pressures require reduction of costs, elimination of waste, pursuit of efficiencies, and measurable patient health outcomes, all of which impact time and limit resources.

Care providers' time to triage and treat patients is more limited and precious than ever. Even minor delays in patient care workflows can cause major issues with responsibilities such as juggling packed patient visit schedules, documenting and coding in the electronic medical record, consulting with fellow care providers, completing surgical procedures, and making inpatient rounds. Authentication and authorization processes that are too complex negatively impact patient care and decrease care provider satisfaction. Maintaining and increasing physician and patient satisfaction is a common strategic goal for healthcare organizations. The Ping Identity Platform can help improve provider and patient experiences, while maintaining security.

In today's interconnected world, patients are also consumers. Factors adjacent to quality of care impact physician and healthcare organization ratings and influence where patients choose to get their healthcare. Healthcare organizations must also provide stellar support for operational functions, such as accounting and revenue cycle, facilities management, and information technology services. Ping Identity offers a platform to provide seamless and secure access to critical clinical and business systems and information, positively impacting patient and care provider satisfaction.

Business Associates of Healthcare Providers

A diverse range of business associates of healthcare organizations can be entrusted with sensitive data such as protected health information (PHI) and personally identifiable information (PII), and

are subject to HIPAA security and risk management expectations. Payors must collaborate with healthcare providers for case management and utilization review, which often leads to requests for direct access to health plan member electronic medical records. Laboratories handle sensitive PHI and utilize shared devices and workflows.

Likewise, pharmaceutical companies handle PHI from human subject research during clinical trials, in addition to proprietary corporate data. Medical device manufacturers are challenged to comply with the HIPAA Security Rule, as well as Food and Drug Administration requirements while providing cost-effective and nimble systems that easily interface with clinical systems and processes, such as electronic medical records, imaging systems, patient monitoring, medication reconciliation and administration, and provider workflow. The Ping Identity Platform facilitates collaboration and partnership with healthcare organizations, which require secure identity and access management to streamline workflows and comply with regulations.

Addressing Concerns of the Healthcare Chief Information Security Officer (CISO)

Healthcare CISOs must balance information security, risk, and regulatory requirements with the availability of clinical and business systems and data. They must deliver authentication workflows and other security controls for internal operations, as well as accommodate collaboration and data sharing with external parties. The healthcare CISO is just as concerned about inhibiting patient care and negatively impacting care provider satisfaction with authentication and other security controls as protecting the organization from breach.

Healthcare CISOs juggle multiple competing priorities, such as preventing and limiting exposure from security incidents and breaches of PHI; minimizing negative impact to patient care and provider satisfaction from security controls; complying with regulatory requirements; and managing risk. The Ping Identity Platform addresses each of these priorities to help a CISO sleep better at night.

Preventing Security Incidents and Breaches

Compromised credentials and unauthorized access to systems and data present risk of security incidents and breaches. Ping Identity's multi-factor authentication (MFA) solution, PingID, adds an additional layer of security such that a compromised user ID and password will not lead to unauthorized and malicious access.

Avoiding Unauthorized Use of Compromised Credentials

With phishing and malware presenting an ever-increasing risk of compromised user credentials, CISOs must ensure that compromised credentials may not be used by an attacker. PingID (MFA) offers multiple authentication options beyond ID and passwords, including:

- Fingerprint and other biometric scanners
- Smart card integration requiring wipe, insert, or tap of smart card
- SMS/MMS text messaging to smartphones

- Mobile app push notifications to smartphones
- Hard tokens

Protecting Organizational and Employee Financial Data

In addition to safeguarding PHI, the Ping Identity Platform protects financial data and PII from unauthorized access. Threats of phishing and compromised credentials increase the risk of exposing sensitive PII or financial data, authorizing malicious funds transfers, and the rerouting of paycheck direct deposits to the accounts of criminals.

PingID enables multi-factor authentication (MFA) to prevent unauthorized user access to financial and HR systems if user credentials are compromised. Ping Identity's web and API access management solution, PingAccess, secures resources at the URI and transaction level to prevent malicious activity surrounding employee PII and financial data. Ping Identity's data access security solution, PingDataGovernance, provides granular access permissions at the data layer, further reducing the risk from insider threats and unauthorized access by compromised credentials.

Securing Access to Web Applications and APIs

Healthcare utilizes legacy and modern web-enabled applications, such as patient portals; online patient survey systems; registries; research and quality improvement data collection and analysis tools; and data warehouses to support business and clinical operations, clinical research, and operational activity. Internet-accessible web applications face risk of unauthorized access. The complexity and on-premises requirements of legacy web access management (WAM) systems and the single-use nature of API gateways leave healthcare enterprises stuck in the middle.

Enter PingAccess, which provides access management by centrally managing authorization capabilities and secure applications and APIs in any domain, for users in any location. PingAccess (Access Management) provides the security and comfort of knowing that only the right users can access sensitive data and resources. A comprehensive policy engine ensures that users are signed on with the appropriate authorization down to the URL level, which provides a more granular level of security via page level access control to sensitive web forms and data. Administrators can customize access policies based on user attributes such as groups, location, time or device, providing centralized and scalable user access control.

HIPAA Security Compliance

The HIPAA Security Rule, as updated by the HITECH component of the American Recovery and Reinvestment Act and Omnibus Rule, defines defensive in-depth controls, including user identification and authentication requirements among administrative, physical, and technical safeguards for PHI. Ping Identity's identity federation and single sign-on (SSO) solution, PingFederate, and PingID (MFA) provide scalable and secure user authentication throughout the environment, helping to ensure that there are not exceptions to authentication policy requirements.

The Ping Identity Platform provides IAM solutions that contribute to satisfying the following specific security safeguards required by the HIPAA Security Rule:

- 164.308(a)(3) Workforce Security Access Authorization
- 164.308(a)(3) Termination Procedure
- 164.312 (d) Person or Entity Authentication

HIPAA Security Risk Management

The use of compromised credentials and dormant yet active accounts of terminated users are threats identified in most healthcare risk analyses, as required by HIPAA Security Rule 45 CFR 164.308(a) (1)(A). PingID (MFA) reduces the risk of remote attackers utilizing compromised user IDs and passwords by requiring another factor of authentication as part of a comprehensive risk management strategy, which is required by HIPAA Security Rule 45 CFR 164.308(a)(1)(B). The risk of not quickly disabling the access of multiple, disparate accounts of terminated users can be remediated with PingAccess (Access Management) ability to quickly revoke all access for specific users across the enterprise.

Care Provider Satisfaction with Security Controls

CISOs must ensure that security controls interfere as little as possible with patient care and provider workflow. Security controls such as authentication, web browsing filtering, anti-malware, and whole disk encryption can cause complexities and delays for care providers when issues arise. PingFederate (SSO) helps removes potentially burdensome authentication requirements with flexible authentication options that accommodate care provider workflow.

Securing and Supporting Patient Portals

Patient and care provider satisfaction, Meaningful Use (MU) requirements, grant funding, and limited resources require the use of web-enabled patient portal access to electronic medical records to provide streamlined communication and coordination between care providers and patients.

Ping's identity and access management solutions integrate with Active Directory and offer an alternative utilizing PingDirectory, a high-scale, high-performance identity management solution, to manage patient portal user accounts, passwords, and authentication policies. PingID (MFA) provides must-have authentication methods that are intuitive and easy for patients to use—via their smartphones—to prevent unauthorized parties from accessing PHI through electronic medical record patient portals.

Payment Card Industry Data Security Standard (PCI DSS)

Healthcare organizations that process credit card transactions for payment include revenue streams like hospital cafeterias and gift shops, patient co-pays, continuing education, and use of conference space, all of which present requirements to comply with PCI DSS. PingID provides another authentication factor beyond user ID and password for administrative access to

Cardholder Data Environments (CDE) and for administrative interactions with point of sale terminals in compliance with PCI DSS.

NIST 800-53A and HITRUST

Health and Human Services and NIST SP 800-66 Guidelines for Implementing the HIPAA Security Rule provide guidance that HIPAA-covered entities should reference NIST SP 800-53A to understand granular controls that are appropriate for implanting HIPAA security safeguards for systems that store or handle ePHI. The Ping Identity Platform maps to the following controls objectives from NIST SP 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations:

- AC-3(2)[1] the organization defines privileged commands and/or other actions for which dual authorization is to be enforced; and AC-3(2)[2] the information system enforces dual authorization for organization-defined privileged commands and/or other organization-defined actions.
- C-3(4) ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL ASSESSMENT OBJECTIVE: Determine if: AC-3(4)[1] the organization defines discretionary access control policies to be enforced over defined subjects and objects;
- AC-3(4)[2] the information system enforces organization-defined discretionary access control policies over defined subjects and objects where the policy specifies that a subject has been granted access to information and can do one or more of the following:
  - AC-3(4)[2](a) pass the information to any other subjects or objects;
  - AC-3(4)[2](b) grant its privileges to other subjects;
  - AC-3(4)[2](c) change security attributes on:
    - AC-3(4)[2](c)[a] subjects,
    - AC-3(4)[2](c)[b] objects,
    - AC-3(4)[2](c)[c] the information system, or
    - AC-3(4)[2](c)[d] the information system's components;
  - AC-3(4)[2](d) choose the security attributes to be associated with newly created or revised objects; or
  - AC-3(4)[2](e) change the rules governing access control.

The Ping Identity Platform also maps to the following two HiTRUST Common Security Framework controls:

- 01.p Secure Log-on Procedures
- 01.q User Identification and Authentication

Addressing Concerns of the Healthcare Chief Information Officer (CIO):

CIOs must focus on delivering scalable and cost-effective information technology infrastructure and applications with limited resources to support their healthcare mission. Technology and security controls must accommodate IT standards and support clinical and business workflows of

clinical and business end users. With PingDataGovernance (Data Access Security) device and attribute-based policy control, a CIO can avoid one-size-fits-all authentication controls and workflows, and tailor security requirements to specific attributes that balance security requirements with associated risk. PingFederate (SSO) offers authentication mechanisms which allow for corporate Active Directory user accounts to be kept separate from external users, if preferred, and the ability to connect users among affiliated and partnered organizations. Whether hosted on premises, at an affiliated institution, or in the cloud, the Ping Identity Platform removes barriers to accessing the data that is critical to research.

Technology that Enables the Healthcare Mission

Electronic medical records, medical devices, data analytics systems, and facility systems are among the many technologies that CIOs must deliver, all while satisfying the CISO and security team's requirements that systems are secure. Ping Identity provides solutions to ease the burden of authentication infrastructure and support, while accommodating clinical and business workflow. As a result, CIOs can focus on delivering the technology that today's complex healthcare environment demands.

Manageable and Standard Technology Infrastructure

Healthcare CIOs must ensure that healthcare technology is reliable, as system issues and outages can jeopardize patient care and safety. Scalable solutions that follow industry standard technology components and protocols are required for the highly available systems that healthcare demands. The Ping Identity Platform is built on open standards to enable any required identity management and authentication use case.

PingAccess (Access Management) accepts secure REST and SOAP-based services using SAML, OAuth, OIDC, WS-Fed, and WS-Trust. These provide authentication integration points between onsite and remote users and disparate clinical systems, bringing them together under central authentication for smooth care provider workflow. It also includes numerous out-of-the-box adapters, agents, and token translators that make it easy to integrate with existing applications and authentication systems. By enabling secure digital partnerships and allowing third-party APIs to access application and resource information, PingAccess ultimately improves productivity for clinicians and the organizations that they collaborate with.

PingAccess can be deployed on premises or in public or private clouds to protect all organizational assets, no matter where they're hosted. This can help accelerate an on-premises or cloud-first strategy and scale to tens of thousands of transactions per second with advanced clustering and replication.

Flexible deployment options include agent and gateway models to meet different healthcare needs. A gateway model can provide access control, web session management, and identity-based auditing centrally, while an agent-based model can be deployed on servers without requiring network or infrastructure modifications. You can deploy gateways, agents, or

both, and they can be used on premises or in the cloud, on diverse platforms including IIS, Apache, NGINX, and F5.

Reasonable Authentication and Security Controls

Healthcare CIOs must strike a balance between supporting the CISO in securing healthcare systems and PHI, while also advocating for care providers that security and authentication controls must be reasonable and enable patient care. A one-sized-fits-all approach may result in either too lax or too stringent authentication controls based on the risk of the data accessed and the circumstances of access.

PingDataGovernance (Data Access Security) provides centralized, fine-grained policy control over access to stored identity and profile data, requiring appropriate levels of authentication based on specific use cases. Healthcare organizations can restrict internal and external applications from accessing specific attributes or entire identity profiles. Device and attribute-based user authentication policies can help adhere to privacy regulations and corporate mandates by restricting access to identity and profile data based on user consent, the requesting application, and even external data sources.

PingDataGovernance allows healthcare CIOs to remove authentication barriers when appropriate, while satisfying the CISO that risky access use cases will require stricter authentication requirements to prevent unauthorized access to systems and data. It offers granular user authentication policy control for clinical systems based on the following variables, providing authentication requirement flexibility:

- Type of device connecting
- New device
- IP range
- Rate limiting
- Group membership
- OS version of device connecting
- Application or resource
- Location
- Last login
- Browser utilized
- Day of week and time of day
- Risk-based authentication (RBA) with other partners

Federated Identity Management in Healthcare

Healthcare organizations, business associates, and agencies must collaborate and communicate for purposes such as treatment, payment, human subjects research, quality improvement, and public health reporting. Health information management functions must be enabled to provide nimble access to patient records to multiple internal and external parties.

PingFederate (SSO) provides the ability for healthcare organizations to:

- Create a secure, scalable, and efficient clinical network by federating to any size partner.
- Grant or revoke secure access for your partners without the cost of managing their credentials.
- Shore up security for your sensitive information by eliminating passwords.

Proven standards-based federated identity management solutions that use identity industry standards, such as SAML, WS-Trust, and OAuth, support a comprehensive IAM plan and provide many benefits to healthcare organizations, including:

- Increased Security
  Password proliferation is reduced to help limit the number of clinical applications requiring separate credentials. Standards-based solutions alleviate the need to replicate, hide, or synchronize passwords, while minimizing the labor and costs related to support.

- Reduced Compliance Risk
  Using token-based secure authentication can eliminate PHI exposure. Centralizing policy and support for all web-based apps allows users to eliminate the effects of password and policy changes, and to simplify the de-provisioning process through existing organizational directories.

- Improved User Productivity and Satisfaction
  Users have access to any web-based application with a single credential, increasing organizational efficiency and user satisfaction, while decreasing IT resource time and budget spent on password resets.

- Easy Deployment
  Integration with existing healthcare IT infrastructure and investments are accelerated, as is connection with MFA providers. Costly, one-off projects are minimized by using supported integrations and standards to avoid fragile or high-maintenance architectures.

- Scalability and Reliability
  Performance-tested, enterprise-grade solutions eliminate the encumbrance of complex deployment, poor support, or lack of dependability.

Electronic Signatures

21 CFR Part 11 prescribes the requirements for determining whether electronic signatures are considered trustworthy, reliable, and equivalent to paper signatures. PingID (MFA) provides the ability to utilize electronic signatures, while accommodating business and clinical workflow. The

Ping Identity Platform meets the following controls required by 21 CFR Part 11 for electronic signatures, which are useful for signing of orders in electronic medical records:

- Ensure that the signer cannot readily repudiate the signed record as not genuine.
- Limit system access to authorized individuals.
- Use operational system checks to enforce permitted sequencing of steps and events, as appropriate.
- Use authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Meaningful Use (MU) of the Electronic Medical Record

ARRA and HITECH provide financial incentives for "meaningful use" of electronic medical records by eligible providers and hospitals. If healthcare organizations meet certain criteria as defined by meaningful use core measures, they can receive direct financial compensation from the U.S, federal government. MU Stage 2 includes security requirements and "core measures" that must be satisfied for organizations to receive and keep funding provided from the MU program. The Ping Identity Platform helps to satisfy Meaningful Use Stage 2 Core Measure 9: 170.314(d)(1):

- Verify against a unique identifier that a person seeking access to electronic protected health information is the one claimed.
- Prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.

Addressing Concerns of the Chief Medical Information Officer (CMIO)

Enabling Clinical Workflow

"I can't tolerate one more mouse click or keystroke in my day" laments many a care provider, frustrated with increasing authentication controls in the clinical systems environment that are necessary in an ever-increasing cyber threat landscape. Some actions in the electronic medical record are so sensitive that reauthentication is required. However, pausing clinical care to authenticate to electronic medical records and other clinical systems multiple times throughout a shift is burdensome.

The Ping Identity Platform provides secure, streamlined authentication to enable outpatient and inpatient care providers to focus less on jumping through hoops of authentication controls and more on patient care. PingFederate (SSO) allows physicians to authenticate once at the beginning of each workstation session, automatically passing credentials to multiple applications without requiring multiple logins. PingFederate and PingID (MFA) integrate with smart card readers and biometric authentication devices to support quick, easy, and secure access to clinical systems. Ping Identity's software development kits support integration with electronic medical records to support granular authentication requirements for Computer Physician Order Entry (CPOE) and

Electronic Prescription of Controlled Substances (EPCS) without requiring slow and antiquated re-authentication with a user ID and password.

Academic Medical Centers

Academic medical centers are among the most complex organizations in healthcare, challenging a CMIO to advocate for high quality healthcare with limited resources. The range of requirements includes:

- Treatment
- Payment
- Operations
- Teaching of medical students
- Managing resident physician rotations
- Quality improvement
- Research
- Public health
- Reporting to registries
- Telemedicine
- Coordination with other healthcare organizations and agencies

Addressing these many functions requires nimble identity and access management processes. Faculty at university schools of medicine often must navigate disparate security controls and authentication requirements for their own hospitals, plus multiple affiliated organizations. Academic medical centers typically utilize multiple onsite and offsite databases and data warehouses to support human subjects research and quality improvement. Research grant funding includes complex reporting requirements and utilization of externally hosted systems, as well as sharing data and allowing access from external principal investigators and research assistants. The Ping Identity Platform provides the ability for affiliated healthcare organizations to provide seamless authentication and access to systems and data for care providers that access disparate networks and systems.

Care Provider Satisfaction

CMIO performance is often measured by physician satisfaction with healthcare technology, along with collaborating with the CIO, CMO, and care providers to ensure the tracking of metrics required as part of meaningful use directives, health plan reimbursement, grant funding, and public health activities. The Ping Identity Platform assists in removing authentication barriers, while ensuring secure access to support healthcare organizations to share data both internally and externally.

Conclusion

Healthcare is a complex environment with many pressures. To contain the rising cost of healthcare, authentication solutions that are scalable, standard, and easy to implement are necessary.

The Ping Identity Platform manages and secures user identity and access to sensitive data, ensuring compliance with a growing range of HIPAA and security requirements. Built on open standards, it provides flexibility, enables clinical and business workflow, and facilitates inter-organization collaboration. Purpose built to address the many diverse needs of healthcare organizations, the Ping Identity Platform ensures security and compliance, while providing the seamless access healthcare professionals, employees, patients, and members demand.

To learn more, visit www.pingidentity.com.