Executive Overview

The web, mobile devices and social networks have drastically changed the way industry works. Hospitals and other healthcare providers are no exception. Doctors, clinicians, hospital staff, affiliated organizations and their partners need secure access to a growing range of healthcare applications — from anywhere and on any device. The support of secure, web-based solutions allows users to easily switch between applications, as well as to send and receive information to relevant, qualified stakeholders. As the healthcare industry evolves, IT leaders must revisit traditional methods for managing both on-premises and web-based identities.

It is crucial for healthcare organizations to consider usability and access within their identity management infrastructure as they embrace mobility and the hybrid cloud. For many healthcare providers, such as hospitals, not only do employees have access to confidential and protected health information (PHI), so do non-employees such as contractors, residents and interns — creating pervasive system access insecurity and tedious work for IT as they closely monitor the systems that employees and non-employees have access to.

Providers need the support of interoperable systems that provide access to readable data across devices and organizations. Proven standards-based identity solutions open a new pathway to establish healthcare interoperability, meet HIPAA and Meaningful Use (MU) requirements and simplify workflows.

This paper explores important security and privacy concerns facing today’s healthcare organizations, including:

1. Converging trends driving complex IT environments and security risks.
2. Ways for healthcare IT professionals to improve identity and access management.
3. The growing applicability of standards-based federated identity solutions.
# Table of Contents

Executive Overview ................................................. 1

Complex IT Trends Driving Access-Related Security Risks .......... 3
  Electronic Medical Records ...................................... 3
  Cloud and Mobile .................................................. 3
  Password Vulnerability .......................................... 4
  Cross Organizational Care ....................................... 4
  Meaningful Use Stage 2 ............................................ 5

Securing a Trusted Information Pathway ........................... 5
  Identity and Access Management ................................ 5
  Internal Audits and Evaluations .................................. 6
  Federated Identity Management Solutions.......................... 6
  The Identity Bridge .................................................. 6

Case Study: How One Hospital Harnessed The Power of Federated Identity Management .............................................. 8
Complex IT Trends Driving Access-Related Security Risks

Information sharing is what defines the digital age. However, for the healthcare sector, information sharing, and all that comes with it, is both a blessing and a curse. With an increased ability to share information comes an increased risk to security.

According to a yearlong study by The Washington Post¹, the healthcare industry is one of the most vulnerable to security breaches in the country. For healthcare IT, meeting or exceeding security, governance and compliance standards is top of mind. Several new IT healthcare trends are converging, making the shift to a centralized approach to identity security inevitable. The top trends pushing the movement include:

- Electronic medical records (EMR)
- Cloud and mobile applications
- Password vulnerability
- Cross-organizational care – ACOs and HIE
- Meaningful Use Stage 2

Healthcare IT professionals are in a difficult position. Driven by the economies of scale that cloud-based solutions offer, healthcare leaders are increasingly pushing IT to deliver more cost-effective and agile ways of doing business. However, supporting the adoption of such solutions and increased collaboration between healthcare providers, both inside and outside the organization, is a complex operation. Choosing the best technology solution to support user needs now and for the future takes time in the midst of ongoing demand.

Electronic Medical Records

According to the Office of the National Coordinator for Health Information Technology² (ONC), electronic medical record adoption rose 33% among hospitals from 2009 to 2012. When integrated with health information exchange (HIE), these electronic and web-based systems allow providers to go beyond organizational walls and securely share information between other hospitals and healthcare providers. The ONC confirmed this momentum, reporting that from 2008 to 2012, health information exchange transactions increased by 41%. Understandably, with this adoption comes many security, compliance, identity and access management concerns.

Cloud and Mobile

There is no doubt that the cloud is penetrating the healthcare sector. Aside from the steady web and cloud migration posing new and growing security challenges for the healthcare enterprise, healthcare professionals are wholeheartedly embracing their mobile devices. According to a study by Manhattan Research³, 85% of the 3,000 physicians polled in the United States use smartphones in the professional setting. Sixty-two percent of US physicians own a tablet, and 50% of these physicians have used their device at the point-of-care.

---


Not surprisingly, physicians who use smartphones, tablets and computers tend to spend more time online than their less-connected peers. Ensuring security and offering robust identity access management solutions requires that healthcare IT leaders consider this trend toward Bring Your Own Device (BYOD) to the care setting.

**Password Vulnerability**

The average employee is tasked with managing between six to 15 passwords daily, and is expected to reset them every 90 days. With such a high volume of password management required, more than 60% of employees reuse their passwords across multiple websites. Unfortunately, this practice of reusing passwords creates the very thing passwords were set up to prevent — breaches.

A recent report by Verizon on cyber attacks on healthcare organizations found that from 2011 to 2012 72% of security breaks were caused by hackers guessing, or using automated systems to guess, the passwords and other credentials to gain access into systems. Therefore, when passwords are recycled or are used across multiple systems, a hacker's success rate increases dramatically. With data breaches costing an average $5.5 million dollars each, and HIPAA making them punishable by law, the stakes are high.

Unfortunately, the negative impact of numerous passwords doesn’t stop at security risks. Today, between 10% and 30% of all help desk calls are for password resets—amounting to as much as $147 per password reset in labor costs alone. Additionally, password issues also persist with managing user provisioning for on-premises and web-based systems as employees join and leave the organization.

**Cross Organizational Care**

Healthcare in the United States is becoming more collaborative and integrated. Models, such as Accountable Care Organizations (ACOs), build collaborative teams of doctors, hospitals and other health care providers who volunteer to give coordinated, high-quality care to the patients they serve — often crossing organizational boundaries, and reinforcing the need for a secure, interoperable healthcare IT system.

Providers want easy access to relevant patient information and the ability to communicate with stakeholders across the care continuum. The industry is actively pushing for ubiquitous health information exchanges (HIE) that will allow clinicians to work together across organizational and geographic lines on the patient’s behalf. HIE provides the technology backbone for collaborative care models, such as ACOs, by integrating disparate datasets to give providers a complete view of the patient’s medical history.

To support initiatives such as HIE and service models like ACOs, healthcare IT must improve the accessibility of patient information while maintaining its security — a difficult yet important balance.

---

6 See footnote 4
7 See footnote 4
Meaningful Use Stage 2

When Meaningful Use Stage 2 took effect in October 2013, the healthcare industry took an important step toward industry-wide interoperability based on common data exchange standards. Such data standards require hospitals to increase inter-organizational connectivity, heighten security and ensure ease-of-use within today’s complex IT environment. However, interoperability will only improve provider workflow when technology systems are protected and streamlined.

In choosing the best solution to support interoperability and inter-organizational connectivity, covered entities, such as hospitals and clinics, need to know what access policies and procedures are in place to address regulatory requirements, including adherence to the access controls and the minimum necessary standard. They should evaluate web and cloud-based vendors for access controls and associated risks. Additionally, they ought to seek vendors that have demonstrated maximum-security readiness to the Office for Civil Rights (OCR) and other internal and external audit entities.

Securing a Trusted Information Pathway

With such high risk and cost associated with identity management, one of the top priorities for healthcare organizations ought to be identity management, especially as they move more into the cloud. Providers need to grant and revoke user access to all critical systems quickly and easily, especially in settings where patient data privacy is vital. To help accomplish this, organizations should:

- Create a comprehensive identity and access management (IAM) plan, starting with internal audits and evaluations.
- Deploy IAM-supporting solutions, such as federated identity management solutions, to streamline business processes, improve agility and increase user satisfaction.
- Integrate an identity bridge solution to securely link between the on-premises environment and web-based applications.

Identity and Access Management

Research analyst firm Gartner defines identity and access management as the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.

Healthcare IT organizations must ensure that they create an IAM strategy that includes an approach for access control today while accounting for the acquisition and adoption of new web and cloud-based applications and tools down the line. It is not only far more cost-effective and risk balancing to proactively build foundational capability for increased web and cloud services; it is a new healthcare security imperative that can no longer be postponed.
Internal Audits and Evaluations
Building a foundation for security, compliance and trust is key for effectively managing and controlling system access. Therefore, security risks must be addressed up front. The critical first step is evaluating authorization levels, application and access levels, and devices used. Additionally, organizations must identify all of their business associates, including those defined by the new HIPAA Omnibus Rule, with access to health records and patient data. They should also perform a risk assessment in order to understand their users, use cases and security risks.

After conducting a robust risk assessment, healthcare organizations should plan for a comprehensive access control strategy. This should include the adoption of SSO and federated identity to secure compliance and reduce risk for both internally and externally hosted systems and users.

Federated Identity Management Solutions
Proven standards-based federated identity management solutions that use identity industry standards, such as Security Assertion Markup Language (SAML), WS-Trust and OAuth, support a comprehensive IAM plan and provide a number of benefits to healthcare organizations, including:

- **Increased Security.** Password proliferation is reduced to help limit the number of 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.** Speed up the integration with existing healthcare IT infrastructure and investments and connect with multi-factor authentication (MFA) providers. Minimize costly, one-off projects 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.

The Identity Bridge
While healthcare organizations still need to provide solutions for on-premises client server applications and shared clinical workstations, there has been a decline in the overall market for single sign-on (SSO) products due to the adoption of newer, more flexible and scalable identity bridge solutions.
Enterprise SSO technology is a traditional tool used in healthcare environments. It automatically logs users into applications via proprietary password replay technology. However, this technology has significant limitations, such as it requires client software, is fragile to application changes, limits usability for offsite users, works poorly or not at all with mobile devices, and exposes application passwords over the network.

Robust enterprise identity bridge solutions deliver the missing link between the on-premises environment and web-based applications — providing SSO from the user’s desktop login to cloud-hosted systems.

Identity bridge solutions are key for improving security and providing a smooth user experience to information networks. Several factors should go into selecting an identity bridge, including tactical investments for reducing labor costs and streamlining resources related to password and identity management.

Key considerations in selecting a robust and scalable identity bridge include the:

- Ability to manage passwords via self-service password reset (SSPR).
- Direct integration of alternative authentication with target systems.
- Ease of integration with existing identity and application infrastructure.
- Application and API authentication capabilities, including support for mobile devices.
- Availability of web SSO coupled with user provisioning, where appropriate.
- Federated SSO capabilities that provide cross-domain access.
Case Study: How One Hospital Harnessed The Power of Federated Identity Management

A major, specialty hospital in the Midwest, named one of Hospitals and Health Networks Magazine’s 2013 “Most Wired Hospital,” needed help with password management and secure access to cloud applications and online information. Specifically, the hospital wanted to:

- Eliminate multiple logins and passwords for employees and affiliated business associates to access cloud applications.
- Ensure that access was disabled when an employee or business associate was no longer affiliated with the hospital.

The hospital selected Ping Identity® because of the simplicity and speed of installation that it offered. PingFederate®, an identity bridge product offered by Ping Identity, integrated smoothly into their existing identity architecture. PingFederate also offered the ability to easily de-provision and remove access rights for users as needed without compromising security or compliance.

The hospital today reports that, with PingFederate, it benefits from:

- A dramatically improved user experience.
- A reduction of the number of forgotten password incidents.
- Supported HIPAA compliance for access to PHI.

About Meditology Services

Meditology Services LLC is a healthcare-focused advisory services firm with core principles of quality, integrity, loyalty and value. Our executive team has an average of 15 years of consulting and operational experience in healthcare with provider and payer clients nationally of varying size and complexity. We understand the importance of relationships and derive much of our business from a long list of satisfied clients who value the quality of our work products combined with the professionalism, approach, and innovative solutions we bring to our engagements. For more information, visit www.meditologyservices.com.

About Ping Identity | The Identity Security Company

Ping Identity is The Identity Security Company. Ping Identity believes secure professional and personal identities underlie human progress in a connected world. Our identity and access management platform gives enterprise customers and employees one-click access to any application from any device. Over 1,000 companies, including half of the Fortune 100, rely on our award-winning products to make the digital world a better experience for hundreds of millions of people. Visit pingidentity.com for more information.