KuppingerCole Report

WHITEPAPER

by Martin Kuppinger| July 2019

IAM for Healthcare: It's time to act

Healthcare organizations deal with highly sensitive information. They face challenges in complying with ever-tightening regulations, combating ever-increasing cyber risks, and adapting to Digital Transformation. Comprehensive healthcare IAM, beyond pure SSO, helps Healthcare organizations to better cope with these challenges.

by **Martin Kuppinger**
mk@kuppingercole.com
July 2019

Content

Table of Figures

Related Research

Executive View: Identity Automation RapidIdentity – 71203

Leadership Compass: Access Governance & Intelligence – 71145

Leadership Compass: Identity Governance & Administration – 71135

Leadership Compass: Identity Provisioning – 71139

Leadership Compass: Privilege Management – 72330

1 Introduction

The healthcare industry, as with many other industries, is facing change and pressure in the age of Digital Transformation and ever-increasing cyber attacks. While some of the challenges healthcare organizations face are the same as other industries, others are industry-specific, such as Electronic Prescribing for Controlled Substances (EPCS) or the Health Insurance Portability and Accountability Act (HIPAA) regulations in the United States.

In order to protect access to sensitive data and assets, Identity and Access Management (IAM) must become the cornerstone of IT infrastructure in healthcare organizations. Restricting and controlling access requires focused protection, down to the granular level of patient records. A comprehensive IAM solution that goes well-beyond pure single-sign on (SSO) meets this need by supporting all types of users and devices and enabling seamless, yet secure, access to all types of applications and data.

In addition, healthcare organizations need identity management solutions that integrate with major healthcare applications and support the healthcare industry's specific SSO challenges. For example, doctors and nurses who use shared terminals require quick access when switching accounts.

There is no doubt that IAM is essential for healthcare organizations – and when executed properly, successfully mitigates security and compliance risks, supports efficiency in daily work, and enables Digital Transformation across the organization.

Identity Automation is a provider of both on-premises and cloud-based IAM solutions (Identity as a Service), with a specific focus on the healthcare industry. Identity Automation delivers a comprehensive IAM solution for healthcare that spans all core IAM capabilities, including Identity Provisioning, Access Governance, Multi-Factor Authentication, and Single Sign-On. Identity Automation also delivers tight integration into major healthcare industry solutions, such as Epic, Cerner, and Meditech.

2 Highlights

- How IAM helps address the challenges healthcare organizations face today, such as ever-tightening regulations, cyber risks, variable workforces, and Digital Transformation.
- Why the current state of IAM in many healthcare organizations is not sufficient to address these challenges.
- What are the requirements and relevant areas of IAM for the healthcare industry.
- How IAM helps balance risk mitigation and business enablement.
- Identity Automation's IAM approach for healthcare organizations enabling rapidly and efficiently addressing IAM challenges
- Recommendations on executing a comprehensive IAM project for healthcare organizations – beyond pure SSO.

3 The Need for IAM: Cyber Risk, Regulatory Compliance, and More

IAM is essential to the IT infrastructure of healthcare organizations, helping them address their challenges in areas, such as compliance & regulations, cybersecurity, and Digital Transformation. IAM is more than a security technology or technical capability, it supports the organization in adapting to new business challenges and drivers.

The healthcare industry is facing change and pressure in the age of the Digital Transformation and ever-increasing cyberattacks. While some challenges healthcare organizations face are the same as those seen in other industries, many are specific to healthcare. For example, due to the highly sensitive nature of patient data, healthcare is one of the most regulated industries, with healthcare organizations being required to comply with a number of regulations, such as Electronic Prescribing for Controlled Substances (EPCS) and the well-known Health Insurance Portability and Accountability Act (HIPAA). Furthermore, the value of patient records is substantial, making healthcare organization a preferred target for cyber attackers.

To protect access to sensitive data and assets, Identity and Access Management (IAM) must become a cornerstone of IT infrastructure in healthcare organizations. Leveraging IAM to restrict and control access allows for focused protection down to the granular level of patient records. While baseline technologies, such as network firewalls and single sign-on (SSO), are also important, they do not deliver the level of sophistication required to protect information assets in today's healthcare organizations.

IAM must become a cornerstone of IT infrastructure in healthcare organizations to support the ever-increasing need for protecting access to sensitive data and assets.

The challenges healthcare organizations face can be mapped to five areas, for all of which a strong IAM infrastructure is beneficial. In fact, without such infrastructure in place, most of these challenges are impossible to effectively address:

- Compliance & Regulations
- Security
- Organizational & Financial Challenges
- M&A Activity
- Digital Transformation

Compliance & Regulations: Healthcare is one of the most regulated industries. Aside from established regulations, such as HIPAA, newer industry-specific regulations, like EPCS and state-level regulations, like the California Consumer Privacy Act (CCPA), have raised the bar for achieving regulatory compliance. Common elements among many of these regulations are the need for strong authentication and sophisticated access control to data and applications and detailed auditing of user activities. At the same time, healthcare providers must be able to gain rapid access in emergency situations. Thus, well-thought-out emergency access processes that still comply with regulations are also required. IAM provides this foundation for balancing business requirements with the level of security and access control needed to comply with regulations.

Security: While regulatory compliance is a topic that is primarily visible to internal management, governance and security teams, and internal and external auditors, cyberattacks have gained broad public attention over the past years. Today, every individual and organization is a target and potential victim. This is a challenge that every healthcare organization's security team must prioritize, especially when it comes to Ransomware attacks, which have recently plagued hospitals. While cybersecurity must go beyond protecting against Ransomware, this form of malware has generated particularly high levels of awareness and concern throughout the healthcare industry.

Unfortunately, healthcare organizations are still mostly reactive when it comes to security, focusing their efforts on prevention, and to a smaller extent, detection. Firewalls, Intrusion Detection Systems (IDS), mostly outsourced Security Information and Event Management (SIEM), and Anti-Malware solutions are the norm. The goal of these technologies is to prevent attackers from entering the organization. While these solutions are necessary and valuable, they do not protect against internal attacks or address attackers who are already in the system.

Restricting access to sensitive systems and data is crucial, particularly once an attacker is in the system. Even if an account is hijacked, the ability to enforce least privilege access can mitigate potential damage. IAM is not a replacement for firewalls and other security systems, but rather, a complement. For example, an IAM solution can deliver information on user behavior to SIEM systems, which in turn, leverage that information to detect anomalies and trigger alerts and counteractions.

Organizational & Financial Challenges: While both regulatory compliance and cybersecurity are reactive measures healthcare organizations must perform, the organizational and financial aspects can be challenging. However, these aspects also present opportunities to increase efficiency and convenience for the workforce with IAM. By giving only the right access, at the right time and providing an SSO portal, IAM delivers an efficient and convenient user experience, while securing access to systems and data as well.

Healthcare organizations face specific challenges with their highly variable workforce, which includes not only doctors and nurses, but also students, patients, and many other types of users who access systems and data.

Even the number of user types is ever-growing, with complex relationships between them and complex access entitlements.

Consider the case of EMR access for "break glass" situations and who might be allowed to access which information when. Dealing with that complexity in managing identities and access requires a well-thought-out IAM solution that supports healthcare's specific requirements.

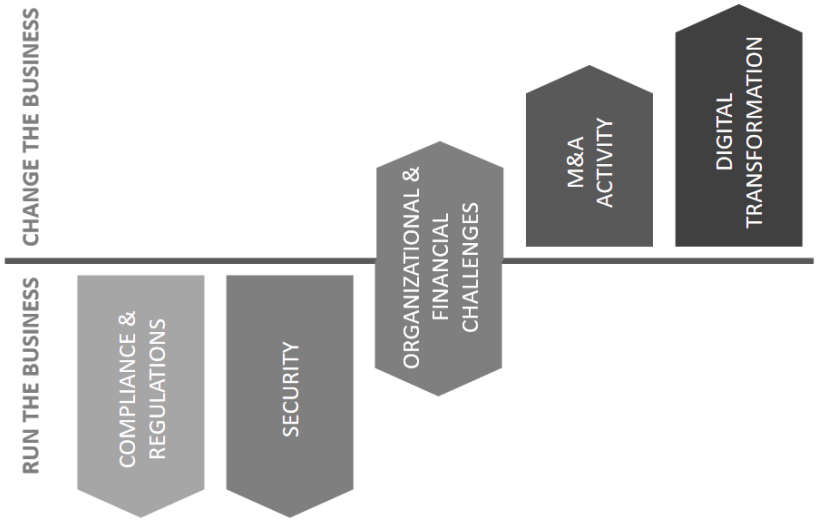


Figure 1: IAM supports healthcare organizations to improve their business while meeting regulatory and security requirements

Like other businesses, healthcare organizations also suffer from challenges, such as limited resources (both human and financial) and a lack of ownership for IAM. If there is ownership, IAM is frequently viewed as a purely administrative IT tool from a technical perspective. However, IAM delivers services to users and the organization that go well-beyond just managing accounts. Ownership must be clearly defined, and projects need support and guidance from adequate sponsors in the organization.

M&A Activity: As many other businesses, healthcare is also subject increased merger and acquisition (M&A) activity. During an M&A, access to the systems of the respective organizations must be managed for both organizations' users. In the near-term, this means the two organizations must federate identities and provide the appropriate level of access to employees, patients, and contractors. However, merging organizations ultimately must also merge IAM infrastructure.

Digital Transformation: Finally, there is Digital Transformation, visible in every aspect of the healthcare organization. Traditionally, healthcare organizations have been challenged with embracing technology evolution. However, increased regulation and overall demand increases, are making this a priority.

Telemedicine, EMR, patient access to information, and the resulting need for Patient Access Management – all require thorough control over an increasing number of identities and an ever-growing number of complex access entitlements. IAM is required to seamlessly support these business processes and ensure they work together. It's about granting the exact level of access required, at the right time, including healthcare-specific use cases, such as controlled emergency access. This requires more than just single sign-on to an application. Provisioning and deprovisioning of accounts, management of access entitlements, audit and governance, and granular access control are all essential IAM capabilities for modern healthcare IT.

The ongoing "consumerization" of digitally delivered healthcare requires organizations to support new groups of users. IT is becoming hybrid – it is no longer about provisioning a single employee or a limited group of users to the Microsoft AD. IAM must support these hybrid environments and multi-cloud infrastructures.

IAM is the foundation for supporting the consumerization of healthcare organizations

Healthcare is, as with many other industries, under pressure from changing business models, technology innovation, and ever-tightening regulations. IAM, specifically an IAM solution that goes well-beyond pure SSO and supports all types of users and devices, is essential to addressing these challenges, while also providing secure access to all types of applications and data.

4 The Challenge: Too much focus on SSO, too little on the rest of IAM today

Today, a significant number of healthcare organizations do not have a mature IAM solution in place, but instead, focus on SSO alone. Unfortunately, SSO is not enough. A comprehensive IAM solution is necessary to meet cybersecurity and privacy requirements. Organizations must view IAM as a business capability, and not just an IT tool.

While there are good reasons for healthcare organizations to have strong IAM in place, the current state of IAM in the vast majority of these organizations is weak. It is estimated that more than 80 percent of healthcare organizations do not have an effective and modern IAM implementation in place, but rather, only have point solutions for cybersecurity, SSO, and possibly, Microsoft Active Directory (AD) management. Simply speaking, although many healthcare organizations have basic identity management and SSO in place, few organizations have reached the next level of IAM. However, more advanced IAM functions, such as granular control over the access of users to systems, data, and even specific data sets, is essential for today's healthcare organizations.

IAM in many healthcare organizations is still a rather technical, administrator-driven set of capabilities, delivered by disparate tools. Instead, the focus should be on an integrated approach that focuses on optimizing user experience and convenience, while also fulfilling the requirements for regulatory compliance and increasing resilience against cyberattacks.

IAM is more than just AD management and SSO – it helps mitigate cyber risks by delivering granular control over access to applications and data.

Legacy approaches, such as using scripts for provisioning new users to the AD, are hard to maintain and rarely deliver a good user experience in terms of fast onboarding and offboarding processes. SSO solutions are necessary, but often lack the granularity needed to provide a secure work environment that protects the privacy of patient records.

The common approach to implementing security, based on policy books, manual processes, and simple manual reports, fails to meet the needs of today. Manual processes are error-prone and cumbersome. The challenge of managing variable workforces, while providing granular access to the appropriate individuals requires tools with a high degree of automation in all identity and access related processes. Moreover, efficient auditing and reporting capabilities are required by many jurisdictions around the world.

In an age of ever-increasing cyber risks, every business struggles with how to best allocate their cybersecurity budget. Frequently, IAM investments appear to be in conflict with cybersecurity expenditures. However, IAM supports both the mitigation of cyber risks, as well as business enablement.

Balancing the different requirements and identifying the right combination of tooling calls for well-thought-out portfolio management that maps the various requirements and optimizes budget allocation. Healthcare organizations need appropriately staffed Information Security departments that have the ability to manage cybersecurity, IAM portfolios, and the underlying program management. This is necessary for not only implementing the tools, but also defining guidelines, policies, and processes.

The focus should be on comprehensive, integrated solutions that support major healthcare applications and address healthcare's unique SSO challenges. For example, fast user switching is needed for doctors and nurses accessing jointly used terminals.

5 The Solution: Integrated IAM for Healthcare

While IAM consists of a broad range of capabilities, there are certain elements that are particularly important for healthcare organizations. IAM for healthcare requires setting the focus on integrated solutions that deliver specialized support for healthcare applications.

IAM is not a single technology or tool. Depending on the definition, it spans a wide range of capabilities. A good way to structure IAM is by mapping the technologies to four areas of capabilities:

- **Administration**: The management of users and their accounts
- **Auditing**: Collecting and analyzing logs, applying Segregation of Duties (SoD) controls, etc.
- **Authentication**: Includes capabilities, such as strong authentication, Multi-Factor Authentication (MFA), and SSO
- **Authorization**: Control over which users are allowed to do what in systems and with data

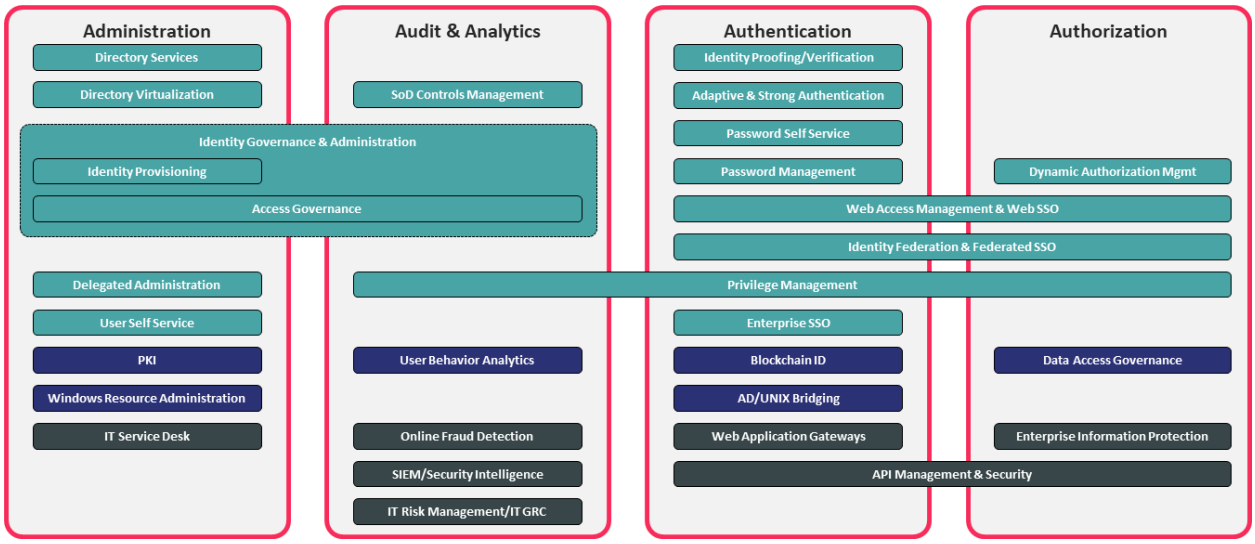


Figure 2: KuppingerCole Reference Architecture for Identity & Access Management

While SSO is essential for healthcare IAM, other capabilities are necessary as well, such as fine-grained access control for EMR, support for MFA, and EPCS support.

In these areas, we find a broad variety of products and services. Beyond the core areas of IAM, such as Identity Provisioning, Access Governance, and SSO, there are other technical capabilities that broader definition of IAM. Furthermore, there are several adjacent areas that overlap or require IAM integration in a mature IT infrastructure. The KuppingerCole IAM Reference Architecture (figure 2) illustrates the breadth of IAM.

For healthcare IAM, the focus should be on:

- Managing all types of identities (users, patients, devices, and applications)
- Provisioning access to target systems and resources governed by fine-grained access control for sensitive data, such as EMRs
- Delivering an SSO experience to users
- Supporting a broad variety of authentication factors for various groups of users, including support for MFA
- Including specialized capabilities for requirements, such as EPCS
- Restricting and controlling access of privileged users
- Auditing and governance capabilities to identify threats, manage risks, and comply with regulations.

When properly integrated, these capabilities ensure healthcare's specific requirements can be met, while avoiding a level of technical complexity that stalls projects. IAM helps organizations balance the usability and convenience required by users to do their day-to-day jobs (such as seamless SSO) with today's security, compliance, and risk mitigation requirements.

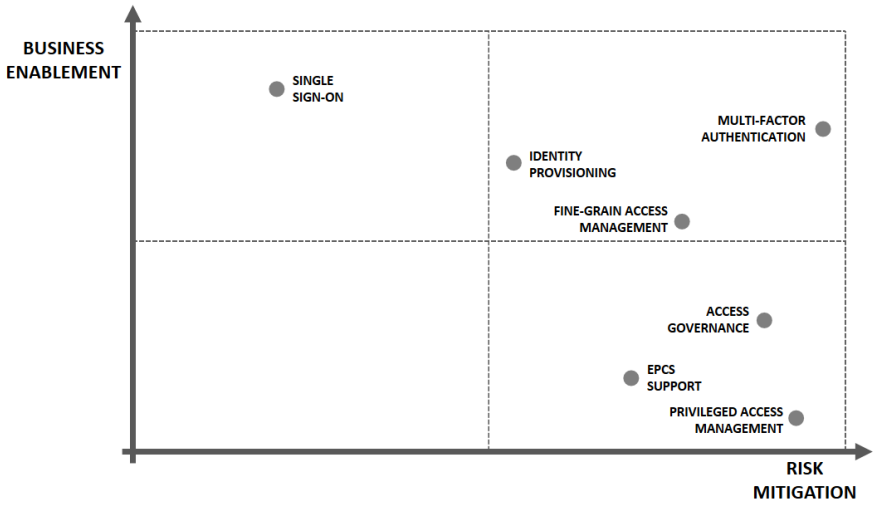


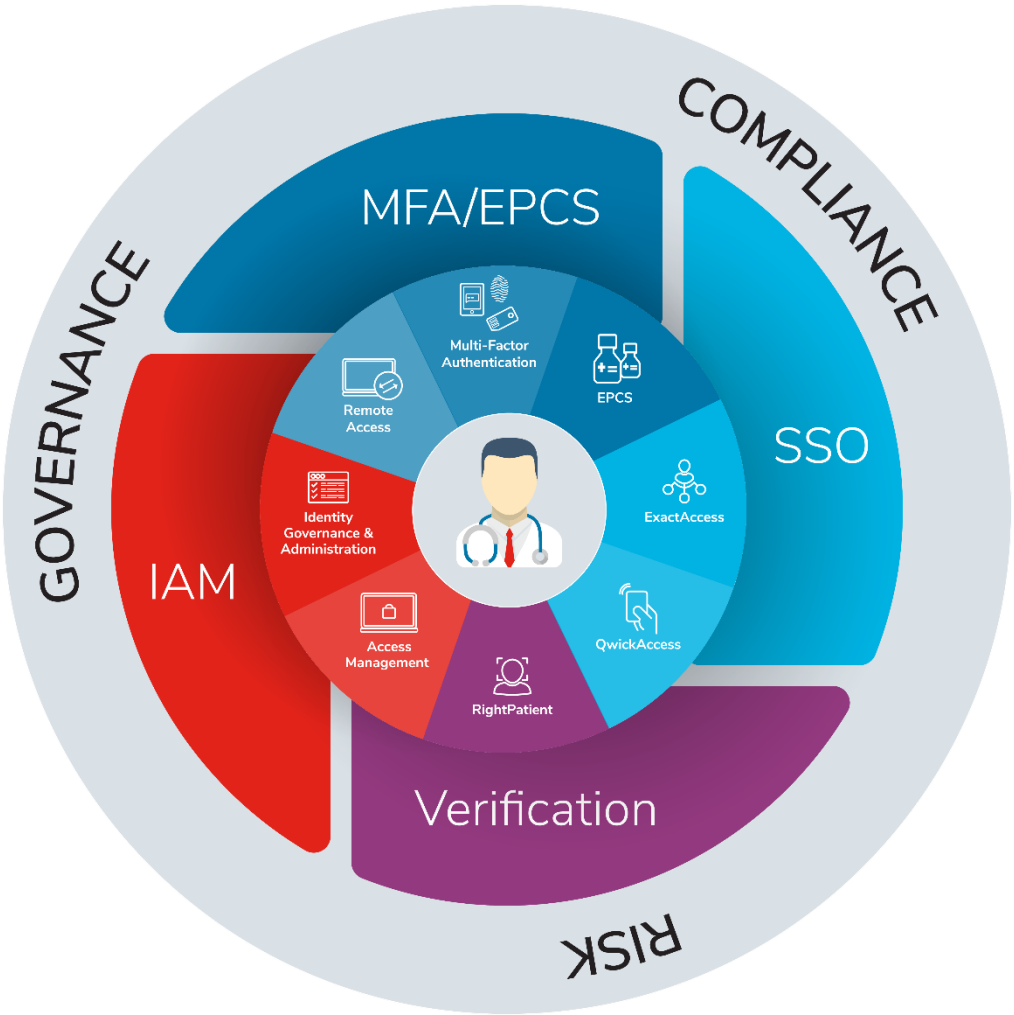
Figure 3: Key IAM technologies for a healthcare IAM solution, based on their impact on Risk Mitigation and Business Enablement

Figure 3 illustrates the impact of the key capabilities of a healthcare IAM solution for both risk mitigation, in terms of security and compliance, and business impact, in terms of usability and support for new requirements in Digital Transformation.

6 The Identity Automation Roadmap to Complete IAM for Healthcare

Identity Automation provides an integrated solution for healthcare IAM, with features and integration that are well-aligned with healthcare's key IAM requirements.

Identity Automation is a provider of both on-premises and cloud-based IAM solutions (IDaaS or Identity as a Service), with a specific focus on the healthcare industry. Back in 2018, Identity Automation acquired HealthCast, an IAM vendor that specialized in the healthcare industry. By combining the two portfolios, Identity Automation now delivers a comprehensive IAM solution for healthcare organizations that spans all core IAM capabilities, such as Identity Provisioning, Access Governance, Multi-Factor Authentication, and Single Sign-On. By leveraging HealthCast's deep roots in healthcare, Identity Automation can also deliver tight integration into major healthcare industry solutions, such as Epic, Cerner, and Meditech.



Figure

Figure 4: Identity Automation focuses on delivering a complete IAM offering for Healthcare (Source: Identity Automation)

This is in direct contrast to niche and point solution vendors that only provide SSO capabilities. With the increasingly complex requirements being put on IAM solutions in the healthcare industry, there is a need for integrated IAM solutions and structured approaches to deliver such capabilities. This integration also helps in efficient implementation and delivery of IAM services in mid-sized organizations, which cannot effectively handle the complexity of a multitude of disparate tools.

With the increasingly complex requirements being put on IAM solutioms in the healthcare industry, there is a need for integrated IAM solutions and structured approaches to deliver such capabilities

Identity Automation focuses its product strategy on five key capabilities:

- Delivering a **flexible** solution with strong out-of-the box capabilities, but still being highly configurable for ad-hoc and complex use cases
- Providing a highly **scalable** offering, both on-premises and in the cloud, that scales well even for millions of identities (users and devices)
- Enabling organizations to manage identities and access in a **secure** way, with a high degree of automation, fine-grained access control, and strong Access Governance capabilities
- Providing a **comprehensive** and integrated solution that supports the major IAM use cases
- Making use of modern Artificial Intelligence (AI) and Machine Learning (ML) technologies for an **intelligent** solution that supports administrators in their role and helps mitigate cyber risks

As a result of the HealthCast acquisition, Identity Automation has increased its existing strength in supporting healthcare requirements by adding a series of specific capabilities, including:

- Single Sign-On support for healthcare-specific applications
- Support for EPCS and SSO auditing
- Drug Enforcement Administration (DEA) compliant MFA
- Tap-and-go proximity badge access to both local Windows desktops and multiple VDI solutions
- Fine-grained access to major healthcare applications
- Connectors to other leading clinical applications for provisioning and auditing integration

These capabilities complement the broad set of features Identity Automation already delivers as part of their offering. These key capabilities include:

- Identity Lifecycle Management, i.e. the ability to manage users and their accounts across systems based on well-defined and automated processes
- Access Governance as the other part of Identity Governance and Administration (IGA), delivering insights into the status and the access risks, while enabling enforcement of the least-privilege principle
- Single Sign-On capabilities, including fast-user switching and integration with Virtual Desktop Application Access, for quick and simple, yet secure access to applications
- Identity Verification features, which allow verification and subsequent authentication of users, including Patient Verification
- Multi-Factor Authentication with extensive support of different authentication technologies, from username/password, to a variety of strong authentication approaches
- Integrated Privileged Access Management (PAM) capabilities to restrict and control access of privileged users, and in general, privilege elevation

When comparing the Identity Automation feature set to what previously has been identified as key capabilities of a healthcare IAM solution, we recognize a strong fit. Identity Automation is delivering these capabilities in an integrated solution, with flexible deployment models and a strong specialization in healthcare and its specific applications, regulations, and requirements.

7 Action Plan for Deploying and Upgrading IAM in Healthcare Organizations

The successful rollout of healthcare IAM requires a defined organization with stakeholders supporting the project with sufficient budgeting, as well as a clearly defined roadmap that breaks the project into phases.

Identity Automation has defined a 24-month roadmap to complete IAM, which is a reasonable action plan for healthcare organizations. While starting with traditional SSO, Identity Automation's plan quickly moves to the more advanced– and mandatory– features, such as automated provisioning and deprovisioning, EMR support, and subsequently, MFA, PAM, and an elaborated Access Governance.

This plan is a well-thought-out concept for delivering quick-wins, while progressing toward a complete IAM strategy in phases.

Successful rollouts of healthcare IAM require a plan that not only delivers visible benefits early, but also reduces complexity by breaking the project into well-defined phases.

Beyond that concrete roadmap for implementing IAM for healthcare organizations, our additional recommendations are:

- Define organizational ownership and responsibility, and identify the stakeholders who must actively support the project and procure the IAM budget
- Clearly separate cybersecurity and IAM, with defined interfaces– to understand where IAM helps in mitigating cyber risks and delivering business benefits
- Define the project, focusing on small steps and on delivering visible improvements (quick wins and big wins)
- Choose the appropriate tooling with focus on well-integrated solutions, delivering specific integrations into the healthcare applications and services in place

IAM is essential for healthcare organizations– and with thorough execution, it will become a success, mitigating security and compliance risks, supporting efficiency in daily work, and enabling the business for Digital Transformation.

8 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Deutschland

Telefon +49 (211) 23 70 77 - 0
Fax+49 (211) 23 70 77 - 11
www.kuppingercole.com