Minimize costs and complexity with AI-powered identity management

Healthcare produces more data than any other industry, but mastering how to use data to be actionable while safeguarding sensitive data from unauthorized access can be a Sisyphean effort. The double-digit year-over-year growth of the medical internet of things (IoT) coupled with a more data-driven approach to patient care is accelerating the volume of sensitive healthcare data that could be vulnerable to misuse or theft. So, it should be of little surprise that traditional forms of identity management lack the agility to keep pace with health IT infrastructure changes.

Fortunately, new forms of identity management leveraging artificial intelligence (AI) and machine learning (ML) can enable health systems, hospitals, and physician practices to remain productive and secure. As healthcare data collection accelerates, the need to safeguard who needs access and when is going to require new levels of sophistication and foresight that some healthcare entities do not currently possess. "In general, less than 3 percent of a health system budget is spent on IT," says Saviynt Vice President of Healthcare Matthew Radcliffe. "Outside of their core clinical, the investment in IT has not kept pace with the speed of growth and expansion, but if we make identity management processes more efficient through the lens of healthcare, healthcare organizations can reprioritize IT resources and invest more in patient care."

> **Less than 3 percent of a health system budget is spent on IT**

For many healthcare organizations, there is a process gap onboarding new clinicians. A lag in enabling clinicians to have data access creates operational inefficiencies that can impact patient care. And while data security is a top-of-mind issue for healthcare organizations, most organizations do not have the security expertise, bandwidth, or know-how to rapidly onboard clinicians seamlessly. "Over the last decade or so, healthcare organizations have come to realize that they need more effective processes to manage access to patient data within enterprise systems by developing an identity governance program," Radcliffe continues.

"To enable a clinician with first-day access to those systems they need—what we call 'birthright access,' the access they need on day one to treat a patient—the sooner they can begin treating patients, the sooner the hospital can realize the operating benefits of a physician/clinician doing their job and the revenue associated with treating patients," adds Radcliffe.

Turning AI into ROI

New forms of identity management enabled by the cloud and powered by AI and ML have the potential to eliminate inefficiencies—such as access gaps that impact clinical and operational workflows—without introducing risks to health data security and privacy.

Process gaps and administrative error can impact clinical and operational productivity and workflows. However, a predictive, AI-driven approach that automates the identity management processes can improve operational efficiencies. The more systems are automated, the level of error and inefficiencies are removed from the process. By removing redundancies, organizations can securely and efficiently give staff access all while improving identity governance. "It's very easy to demonstrate an ROI around productivity and how these solutions can help staff gain access sooner and more securely," explains Gianni Aiello, Director of Product Management at Saviynt. "We have been solving these problems for a long time, but in some cases the way tools were used led to overentitled access that users did not use or need. This was the result of a focus on productivity over security. The outcome was higher risk of a breach and the potential for massive fines. AI and ML approaches can help reduce the potential risk of incorrect access by 10–30 percent while also improving productivity around governing access by up to 60 percent. This represents a huge return for healthcare organizations."

The challenge of present-day identity management is one of bandwidth. "Healthcare is transforming so fast that humans can't keep up with ever-changing user populations, the rapid need for access, and more importantly, the need to govern that access," Radcliffe stresses. "Now consider marrying the transformation challenge with the rapid increase and use of connected devices in healthcare—connected IoT devices, infusion pumps, heart monitors, and smart beds as the most common examples. These connected devices are generating enormous amounts of data, and there's no way a human would be able to respond to these dynamics without leveraging efficient and automated governance platforms." But the use of machine learning for identity management can turn current data into actionable information in two areas: access automation and regulatory compliance.

Healthcare organizations need a convenient way to have staff log on/off of shared clinical desktops, and historically, to authenticate users, most organizations would leverage the "tap in, tap out," single-sign-on method and this is where traditional healthcare-based identity management programs would start and stop. Clinicians were historically enabled with these types of access management solutions without first understanding the specific role the clinician would serve within the organization, determining if the clinician had previous access that could potentially conflict with net-new access, or if the user should even be enabled with access due to some level of security policy conflict. As the number of users and systems have exceptionally grown, there is greater need for healthcare organizations to establish a full identity management program. Innovative healthcare organizations should broaden their identity management program principles by adapting identity governance, data governance, privileged access management, and enterprise single sign-on as a full identity program.

> **AI and ML can help reduce the potential risk of incorrect access by 10–30 percent**

"The amount of data that needs to be collected, and ultimately looked at and analyzed, is huge," says Aiello. "Looking for that needle in a haystack, for a human, is quite frankly nearly impossible. It's just not achievable. And so, machine learning is, in real terms, the only way you can start to better see and understand how people are using their access."

"Unlike early machine learning and AI applications that were mainly rule-based approaches, we're looking at specific scenarios that can be solved by discovered risk not predetermined rules" notes Aiello. "That knowledge can be transferred to how you ultimately model access for the efficiency of staff around what they need to have access to do that job," Aiello states. "Providing snapshots of access is a step toward homing in on appropriate access rights and ultimately determining how to grant and manage access moving forward."

Improving regulatory compliance

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that an individual or entity accessing protected health information (PHI) electronically be authenticated before access is granted. Unlike other industries, health systems, hospitals, and physician practices that have a data breach are often faced with consequences that go beyond significant fines, e.g., an erosion of patient and clinician trust.

Federal and state regulations for reporting health data security and privacy are increasing, and the task of maintaining healthcare data compliance will continue to be a daunting, labor-intensive administrative process that will require consistent organizational commitment and vigilance. By automating access rights and augmenting decisions processes, organizations can leverage their data to help reduce the burden of user compliance.

"At Saviynt, we catalog access that is inherently low risk and doesn't expose data to inappropriate functions or allow for a clinician to see data that's inherently risky to the organization," Aiello reveals.

Automating user access creates a building block for more intelligent decision-making around identity management and governance. As healthcare focuses on their mission of driving operational and clinical efficiencies to improving patient outcomes, an AI-enabled identity management solution can be a strategic investment that can evolve with an organization's current and future IT roadmaps.

Minimize costs and complexity

With a drive toward digitalization, many healthcare organizations are leveraging the prodigious amount of sensitive data for decision-making. When it comes to leveraging data to drive better patient outcomes, healthcare leaders are vacillating between innovation and compliance.

Effective identity management is critical to data governance. As such, healthcare organizations can lay the groundwork to ensuring that increasing data access doesn't lead to exponential growth in risk. "This is a business opportunity for healthcare

> **Automating user access creates a building block for more intelligent decision-making around identity management and governance**

organizations," Radcliffe advises. "The way they see the opportunity to grow their business is to obtain access to more data and more patients beyond the brick-and-mortar hospital. This means broader access to digital records with the aim of caring for patients across the continuum of care."

"We have to infuse integrated identity and data governance platforms into the digitization of healthcare while leveraging AI and machine learning to keep up with the pace of healthcare business transformation," Radcliffe concludes.

To drive operational efficiencies, healthcare organizations should invest in an AI-powered identity management solution for future operational success.

Identity Security for the Cloud Enterprise

Saviynt.com

Saviynt is the leader in identity security for the cloud enterprise. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, ensuring workers have the right access to do their job—no more, no less.

In the United States, KPMG serves over **50 percent of the top 45** pediatric hospitals. We serve almost **60 percent of the top 150 healthcare systems** and **70 percent of academic medical centers.**

- KPMG is a top deployment alliance of Saviynt solutions with a focus on achieving business goals through technology.
- As a Saviynt Delivery Admiral since 2018, we've delivered over 200 engagements, including some of the largest and most complex deployments of Saviynt.
- Our Saviynt implementation methodology is based on industry-leading practices and is continually refined by collaboration between our delivery teams. We strive to learn every day, on every implementation, and to improve our processes continually.

  We've enhanced our Saviynt and IAM implementation methodology through investments in building an extensive catalog of intellectual property, enablers, and accelerators. This helps us design platforms that meet our clients' business needs today and are ready for the future, saving time and money and accelerating long-term ROI.

Contact

Rajan Behal
Managing Director
T: 281-871-9745
E: rbehal@kpmg.com

Debbie Patterson
Senior Director,
Alliances
T: 512-423-6150
E: deborahpatterson@kpmg.com

Aziz Araji
Associate Director,
Solution Relation Alliances
T: 703-863-8812
E: azizaraji@kpmg.com

Scott Jolly
Senior Director,
Solution Relation Alliances
T: 434-242-9485
E: scottjolly@kpmg.com

Sandeep Kaujalgi
Senior Director,
Solution Relation Alliances
T: 415-528-6010
E: skaujalgi@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia