Six essential identity governance capabilities for healthcare organizations

Healthcare organizations use identity governance to keep sensitive clinical data safe by ensuring that users only have access to what they need. At the same time, identity governance facilitates the appropriate access so that staff can carry out their work without delay, especially as they await provisioning, or ongoing interruption such as when their roles change or end.

Six essential capabilities to look for should include:

Self-service access request so that users can apply for access themselves. The access request system provides a single interface for requesting and approving access, while automated policy management boosts security through consistent policy enforcement.

Access certification with artificial intelligence (AI) algorithms to ascertain what kind of access users need. Built-in reporting reduces the cost of compliance by automatically generating audit trails and access reports on all key applications and data.

Connectivity/Integration among applications and data sources. It's not uncommon for a larger health system to have hundreds of applications including EHR and EMR in use. An identity governance platform should integrate them all, be they homegrown or commercial, to accomplish identity-related tasks.

Automated provisioning to applications based on users' roles. Users can be productive from day one, with access changing appropriately as their role evolves. Automated removal of access and accounts, as needed, helps to manage risk.

Centralized ID warehouse you can't manage what you don't know about. For an effective identity governance outcome, having all identities and the access they should have in one place is important. One set of this information that everyone uses reduces the complexities and confusion when determining if access is needed and setting access controls. This reduces time and expense and increases confidence in cybersecurity.

Scalability to accommodate an expanding organization. User experience and processing time remain unaffected with the addition of identities, accounts, assigned entitlements, and applications. The operational health and status of the system is visible, while the system itself is engineered to optimize complicated tasks.

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 partner of SailPoint solutions with a focus on achieving business goals through technology.

— As a SailPoint Delivery Admiral since 2018, we've delivered over 200 engagements including some of the largest and most complex deployments of IIQ.

— Our SailPoint 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 SailPoint 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.

Identity security for the cloud enterprise

sailpoint.com

SailPoint 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.

Contact us

Jim Wilhelm
Principal, Advisory
T: 267-256-7271
E: jameswilhelm@kpmg.com

Debbie Patterson
Alliance Director
T: 512-423-6150
E: deborahpatterson@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