Identity Governance & Administration in Healthcare

Healthcare IT Security and Compliance Whitepaper

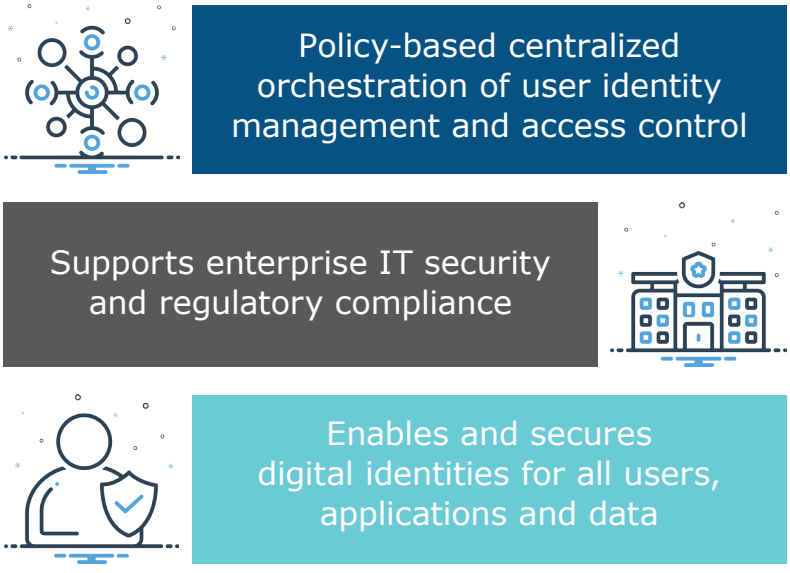
Table of Contents

Executive Summary

This whitepaper is designed as a resource to assist readers in getting started on their identity governance and administration (IGA) journey. There are important questions to ask and factors to weigh before even beginning to consider a software solution. Learn what IGA means, why it is important and what organizations should plan for, understand and anticipate to ensure the selection of the right combination of solutions and services for end users and specific environments.

What is Identity Governance and Administration?

Identity governance and administration is commonly known as centralized visibility of identity management and access controls. These controls should be policy-based and support overall security, regulatory compliance and auditing practices. IGA provides lifecycle management of digital identities, promoting consistent business processes for reviewing, requesting, approving/revoking access and managing passwords, underpinned by a common policy, role and risk model.



IGA provides healthcare organizations with powerful benefits and has adapted accordingly to the industry's cloud-based demands. IGA provides a central location to enable and secure digital identities for all users, applications and data. In a nutshell, it enables the right individuals to access the right resources at the right times for the right reasons.

History Behind the Powerful Benefits & Impressive Growth

There's no doubt about it, IGA is here to stay. IGA is growing at an impressive rate, and changes in the healthcare industry continue to feed this upward trend. It emerged as a new category of identity management driven by mandates and regulatory requirements like Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA) meant to improve transparency and manageability. In fact, IGA was recognized by Gartner as the fastest-growing sector of the identity management market back in 2012 and has continued an upward trend since. That year, Gartner also stated that identity governance "is replacing user administration and provisioning as the new center of gravity for IGA."[2]

Originally predicted to grow at 35-40% per year, it grew to a $3.04 billion market in 2018. Several factors contributed to IGA's growth, including increases in insider theft and fraud, regulations regarding the security of protected health information (PHI), and frequently changing roles and locations of providers and support staff.

Identity Governance and Administration Timeline

Emerged as a new category of identity management driven by the requirements of **new regulatory mandates** such as the **Sarbanes-Oxley Act and HIPAA**.

Recognized by Gartner as the **fastest-growing sector** of the identity management market in 2012.

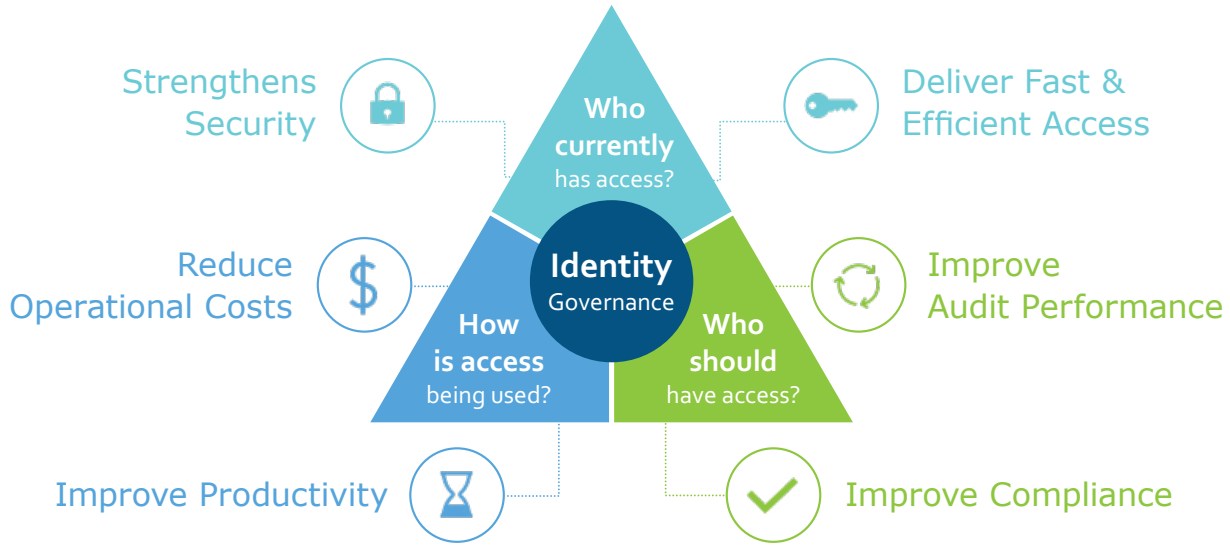
Gartner stated that identity governance **"is replacing user administration and provisioning as the new center of gravity for IGA."**

Gartner estimated **growth rates would exceed 35-40% per year**, based on increased incidences of insider theft and fraud.

2 Earl Perkins, Gartner Magic Quadrant for Identity and Access Governance, (2012).

Benefits of Identity Governance and Administration

IGA empowers organizations to grant end users the access needed to be up and running more efficiently, while also expediting user deprovisioning in the event of end-user departure or termination. This saves valuable time for departments like HR and, especially, IT and reduces the time it takes to grant new employees access to critical systems by eliminating manual provisioning processes that in the past may have caused delays of days or weeks. IGA reduces IT staff workload by providing a centralized, streamlined location for user identity and access management - in both cloud-based and data center scenarios. Not only is security enhanced, but improved reporting protects organizations from non-compliance with industry regulations.



Other benefits of identity governance and administration:

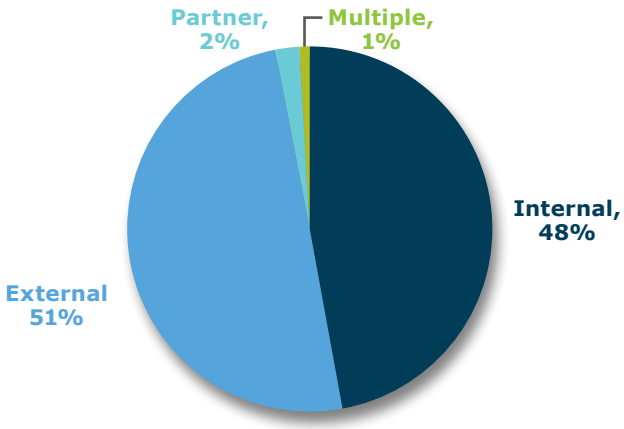
- Delivers efficient access to business users, empowering them to request access and manage passwords
- Reduces operational costs by automating access certifications and requests, password management and provisioning
- Reduces IT staff workload

Why is Identity Governance and Administration Growing in Healthcare?

The HIMSS 2019 Cybersecurity Survey shows that "a pattern of cybersecurity threats and experiences is discernable across US healthcare organizations." Furthermore, the survey states that "almost half (48%) of all respondents cited two primary threat actors; online scam artists (28%) and negligent insiders (20%)."[2]

Healthcare Breaches by Threat Actors[3]

Verizon 2020 Data Breach Investigations Report

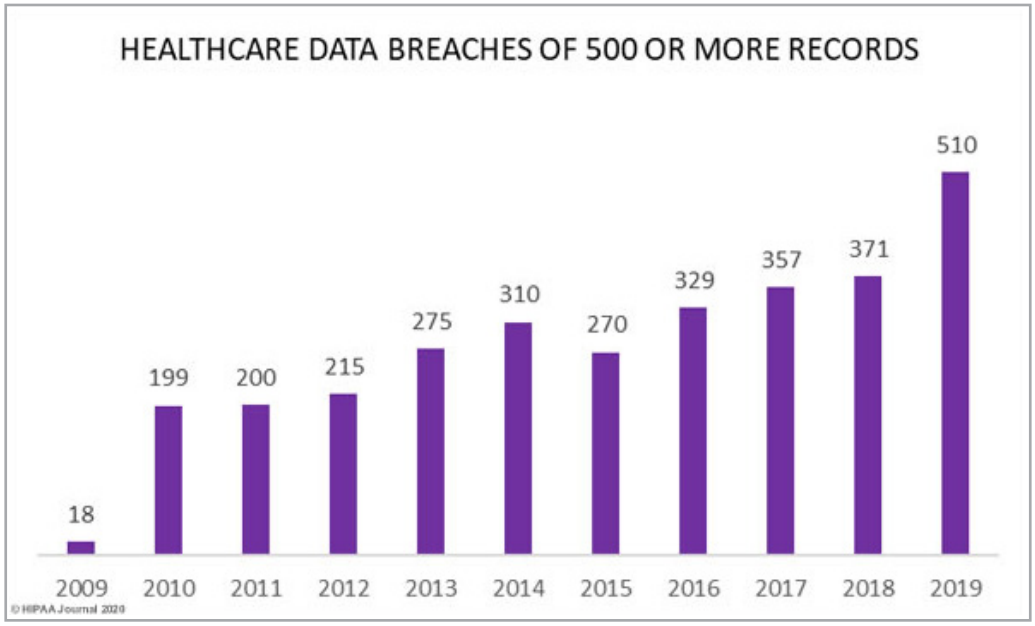


Insider breaches, as these statistics simply outline, continue to force identity governance into the forefront of a security strategy in healthcare just like it has in other industries like financial, energy and government. Additionally, healthcare providers and staff are more mobile than ever – frequently changing locations and roles. These factors, combined with the requirements of regulatory mandates (such as the Sarbanes-Oxley Act and HIPAA), present a clear need for IGA in healthcare.

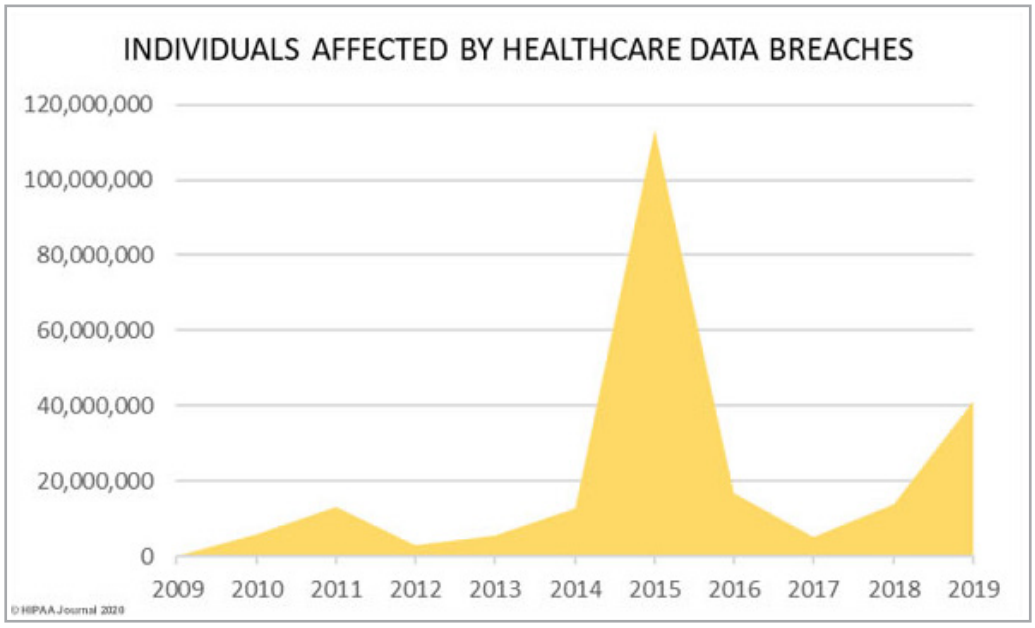
"As with hacking, healthcare organizations are getting better at detecting internal breaches and reporting those breaches to the Office for Civil Rights. These incidents consist of errors by employees, negligence and acts by malicious insiders."[3]

2 HIMSS Cybersecurity Survey, (Healthcare Information and Management Systems Society, 2019), 3 & 6.

3 2020 Data Breach Investigation Report, (Verizon, 2020), 56.



©HIPAA Journal 2020[4]



©HIPAA Journal 2020[4]

4 Healthcare Data Breach Statistics, (HIPAA Journal, 2020).

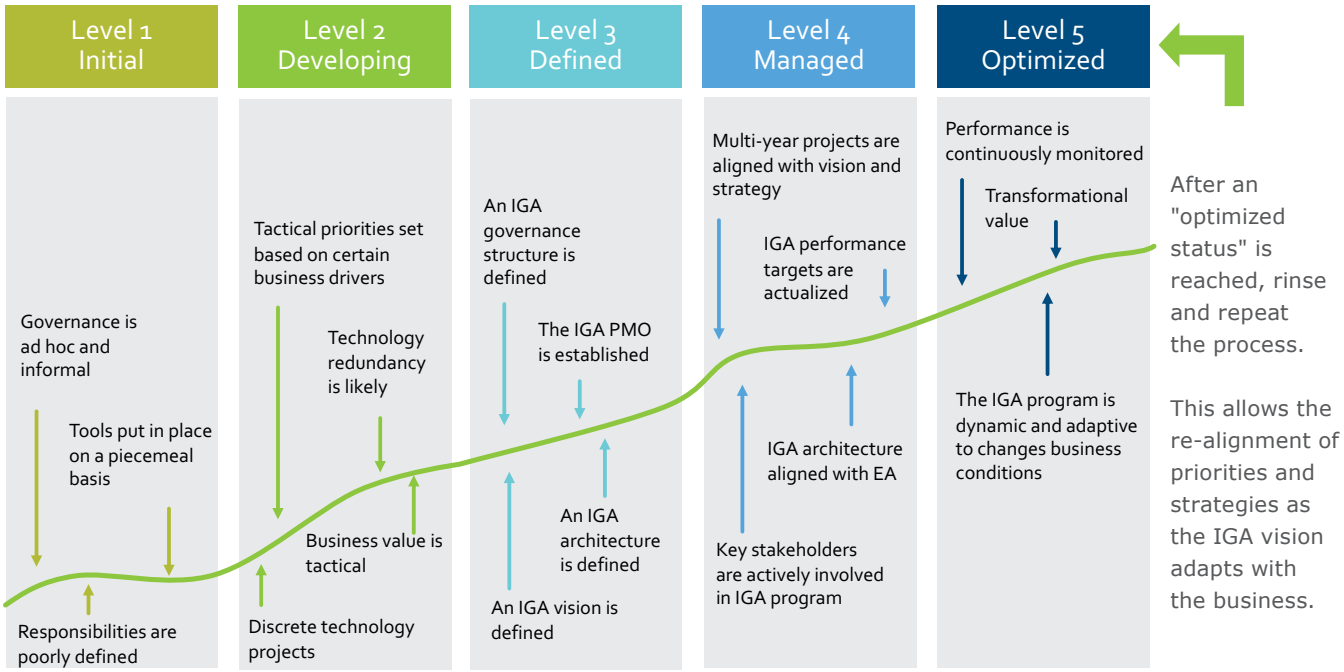
How Should Organizations Determine the Best Approach?

While fully embracing the tenets of identity governance can result in true business transformation, organizations often want to approach IGA as a short-term technical project. The best approach is to plan for the long-term, to consider a fully integrated approach that is continually optimized as it matures, while tackling high-value, clear-vision projects that rapidly provide business value.

It is important to prepare at the leadership level to support managers and staff with implementing and supporting an IGA solution. The following are a few good questions to ask before embarking on an identity project that requires the cross-departmental cooperation and execution of identity governance.

Is there an identity strategy?	Is the current culture supportive of the strategy?	Are there people to execute and maintain the strategy?
• Focus on the future • Guidance for employees • Ownership and accountability	• Culture defines behavior • Culture defines what is important • Culture complements strategy	• Invest in the right team (skills and headcount) • Alignment with the culture

While alignment of strategy and culture are important goals of any organization, there are levels of development and maturity to any strategy. On the next page is a detailed graphic outlining a sample plan for achieving an "optimized" level. Each level builds on the next to grow and maintain a successful IGA strategy.



Upon reaching an optimized level of maturity, organizations will most likely have a shift in strategy, whether big or small. As with all businesses, healthcare organizations must adjust their business to align with such things as acquisitions, recessions, demographic changes, new technologies, and - unique to healthcare - medical treatment options, illness trends and changing regulations. It's important to continually realign the IGA vision and business strategy to ensure organizational security now and in the future.

However, IGA is not a one-size-fits-all solution. The starting point for an IGA strategy will vary and should be developed around the unique requirements and objectives of the organization. The approach of a 200-facility organization with over 10,000 employees operating in multiple states will have fundamentally different goals than the approach of a community hospital with one affiliated physician practice. It’s also very important to recognize that IGA is not one destination or one project, it is a journey or program with risks that are specific to the business. A good tenet of a successful IGA strategy is to ensure a facility's overall security is stronger than it was before the program began.

Here are some quick tips for moving up the levels on the chart from page 8:

1. **Establish an IAM/IGA team.** This is a long-term team that will handle the short-term projects as well as changes in ongoing identity strategy to ensure alignment with the organization's business strategy. They are accountable to the leadership team but are also responsible for maintaining the day-to-day needs of any software and hardware solutions needed to support the identity strategy.

2. **Identify the most immediate risk and tackle it quickly:** This will keep decision makers engaged and show them quick time to value. As mentioned previously, the true benefit is the long-term, but if the leadership team becomes disillusioned or impatient with the program, it could stall. Tackle some short-term projects to show the value of identity governance while building toward optimization.

3. **Staff appropriately.** Don't underestimate the effort required for most organizations to work through the levels of optimization. Tackling the identification of roles, such as nursing, can be overwhelming when viewing HR's list of job descriptions. However, there are best practices and lessons learned available from other healthcare IT professionals, consultants, security firms, continuing education, forums, whitepapers, industry experts and more. Starting from ground zero is not necessary. Reach out to others to see what has worked, but keep in mind that a support team for the project and organization is essential to mitigate risk.

4. **Decision making is cross-departmental.** While IT will most likely own identity governance, it is important to relay value and understand the ROI from other departments early in the process. HR, Operations, Compliance, along with varied departments within IT, are often integral to the decision-making process.

5. **IGA impacts all departments.** It can be a transformative part of rolling out an IGA strategy to transfer access audits to managers, instead of having it sit with IT and department heads. Involve all affected departments on how process changes will affect them. Again, communicating process changes early, especially how auditing will be performed, is integral for mitigating the risk of assigning access to the wrong users.

Case Studies for Identity Governance Success

Although IGA initiatives can have the perception of long timelines and high costs, the benefits can far outweigh the challenges. Review the use cases below to see real-world applications and benefits.

Scenario 1: Quickly Onboarding New Users at New Facilities

Handling the volume of new users as new ambulatory facilities are acquired can be a challenge for many healthcare IT departments at healthcare organizations. Granting the right access to mission-critical applications and ensuring user have the correct access as they move through multiple departments and locations at different times is a challenge when using manual processes.

Implementing a comprehensive identity governance and administration platform:

- Reduces time to provision new user accounts with automated processes
- Provides the right access to users moving among multiple locations
- Reduces risk of a security breach brought on by giving the wrong access to the wrong person
- Reduces the administration burden for IT staff

Scenario 2: Standardize Processes and Policies

Many healthcare organizations have no standard approach for creating and provisioning user accounts. Employees responsible for this function may use their own method during their shift and don't share or cross-train, especially at smaller facilities where only 2-3 employees are handling these duties. Often, important components are left out during account creation or errors are made in the pursuit of expediting the user's access. There is also a risk of inconsistent terminology usage for naming roles, departments or locations.

Rolling out a new identity governance and administration solution:

- Helps reduce errors and inconsistencies
- Standardizes the approach for account creation
- Simplifies provisioning across the health system
- Reduces the risk of an audit failure or non-compliance

Scenario 3: User-Access Reviews

Hospitals often use manual processes to perform user-access reviews and audits by exporting data from multiple applications into spreadsheets. Often, these spreadsheets are then printed out and hand-walked to department heads for review and signatures, sitting on desks until the busy leadership team members have time to review and pass to the next person. There is no way to effectively manage this process or ensure spreadsheets were reviewed in a timely manner.

Implementing an identity governance and administration solution can:

- Automate this process
- Improve accountability with audit scheduling

Scenario 4: Unstructured Data Access

Data Loss Prevention (DLP) can be a substantial problem for some hospitals and it can be difficult to uncover granular-level details about that data. Specifically, where the data is, whether it's active, where the sensitive data is (and how it's accessed and if permissions are used).

There are solutions that can protect and combat "data on the move" that include:

- Access permissions
- Methods for discovering and classifying sensitive data
- Monitoring file access

Scenario 5: Adopting a Cybersecurity Framework

Security frameworks, like NIST or HITRUST, are a badge of honor for hospitals and their IT leadership, and they lower cyber security insurance premiums. Some organizations struggle to check off all the boxes required for compliance. However, identity governance can help achieve a compliance framework that meets the necessary regulatory requirements, specifically:

- Access certifications
- SOD policies
- Protecting access to unstructured data

Scenario 6: New-Hire Access on Day One

On day one newly hired doctors and nurses need access to their critical systems and applications. Often, IT departments have few staff managing the provisioning of many identities and, subsequently, far too much paper. New hires get bogged down with forms to be completed, and subsequent access requests are also filled out manually via paper and walked to the appropriate person.

With an identity governance and administration strategy:

- Accounts are automatically provisioned
- Access requests are conveniently and quickly completed via an online portal

Select a Solution

As mentioned previously, IGA is not a one-size-fits-all solution. There are many industry players with various strengths and weaknesses, but there are common product features that should be a part of any solution. These include:

User Administration	Privileged Identity Management	Identity Intelligence	Role-based Identity Administration	Auditing and Analytics

Questions to ask when choosing an IGA solution include:

- What is the primary objective/issue to address?
- Beyond employees, what other types of users are included?
  - Customers?
  - Vendors?
  - Contractors/consultants?
- What is the covered environment?
  - Physical data centers/virtual machines?
  - Cloud-based assets?
  - Mobile devices?
- How many identities need to be secured?
- How will it be managed – internally, externally or a combination?
- Cloud-based SaaS vs. on-premises solution?
- How well does it integrate?

Conclusion

Because of the value of its identities, the healthcare industry is particularly vulnerable to cybersecurity threats, as well as insider threats. In fact, Forbes has estimated that 58% of all healthcare breaches are initiated by insiders. That's a sobering statistic. The good news is that IGA has the power to enhance onboarding while improving security, reportability, and user identity management – all from a centralized location. No two organizations are the same, including their EHR, other clinical systems, HR process, network, user communities, company culture, data locations, access methods, etc. Project leaders should plan early and ask the right questions about their organization's technical environment but also its readiness and strategy for long-term execution.

Key Takeaways:

- **Start planning now**
- **Assess organizational readiness**
- **Assess the technical environment**
- **Prioritize requirements for a solution and services**
- **Continue to optimize**

Why Forward Advantage?

Forward Advantage has 25+ years of experience in the healthcare industry, working with a variety of EHRs and as a MEDITECH-preferred partner. We offer industry-leading IGA solutions and help each hospital build its own unique strategy based on user communities and environment. It's never too early to start planning for an identity governance program. Contact us for help evaluating your current environment and existing strategies to ensure an IGA solution that fits your needs now and long into the future.

forward advantage

877.636.7927
info@forwardadvantage.com

www.forwardadvantage.com
7255 N. First Street, Suite 106, Fresno, CA 93720