FORTRA

GUIDE (Core Security)

Doing Healthcare Identity Governance Right

The Ultimate Guide For Managing It

Table of Contents

The Ultimate Guide Overview

Healthcare organizations today face extraordinary challenges in a dynamic, complex landscape. During the last two decades, the healthcare industry has seen increasing regulations, an acceleration of technology and workforce growth, acquisitions and consolidation, and the pressure to increase operational efficiencies and decrease overall costs, while meeting growing patient demands. The pressures to comply with increasing regulations, coupled with pressures to compete with other healthcare organizations, also make for a challenging environment. Addressing these issues, while staying focused on delivering quality patient care, means healthcare organizations must continually do more with less.

That's where Identity Governance and Administration (IGA) comes in—enabling healthcare organizations to intelligently and efficiently manage who has access to what systems and when, and empowering healthcare professionals to deliver the highest quality of care possible, while protecting valuable patient data. Throughout this guide, we will explore key issues and trends within the healthcare industry that warrant the need for effective identity governance. We will explore the top five drivers for IGA within healthcare organizations today, and analyze critical healthcare challenges in identity governance. Most importantly, you will receive actionable strategies for leveraging an intelligent IGA program within your healthcare organization to meet ongoing compliance requirements, boost operational efficiencies, and ensure appropriate levels of access within your healthcare environment.

Key Identity Governance and Administration Terms

Provisioning and Deprovisioning: The setting up, removal, or changing of user access to resources and applications.

Access Certification: A process where managers or individuals responsible for administering an application must review users who have access to that application. Commonly known as access reviews, this process includes an attestation that the user still requires, or no longer requires, access to the application. Unnecessary access is subsequently removed.

Roles: A collection of access rights on one or several applications that are grouped together because they are often assigned to the same types of users. When roles are defined, organizations can efficiently assign rights in automated fashion.

The Current State of Healthcare Information Security

Healthcare information security remains a top priority as health systems have adopted modern approaches to storing and securing electronic health information. Healthcare records are extremely valuable because they contain highly sensitive data, including social security numbers, bank information, and personal health information. In fact, a recent study published in the Annals of Internal Medicine, which analyzed nearly 1,500 data breaches across nearly 1,400 hospital facilities, affecting approximately 169 million patients between October 2009 and July 2019, found that 70 percent of breaches targeted demographic or financial information rather than medical information only.

Forbes also highlighted an important finding from this study. Specifically, 'one of the most common ways hackers infiltrate hospitals is [a result of the business] not revoking former employees' login credentials after employment is terminated.' With the rise of digital and electronic health records, healthcare organizations must continue to evolve their thinking and pursue strategies and programs that protect sensitive information across their environments. One of the most effective ways healthcare organizations can secure sensitive information is through effective Identity Governance and Administration (IGA) programs. IGA policies and programs enable the right people to have the right access to the right systems and applications at the right time—for the right reasons.

Key Issues and Trends in the Healthcare Industry

To understand what healthcare organizations are up against today, it is important to more deeply examine a number of top challenges and trends in the healthcare industry. Below are eight key issues that characterize the current healthcare environment:

1. **Growing Cybersecurity Threats and Data Breaches:** Healthcare organizations face unique cybersecurity challenges, including protecting electronic health information (ePHI) and electronic health records (EHR). However, many healthcare organizations may not have the ability to cover all potential risks to protect sensitive information, and must balance the cost of protecting the organization with delivering quality, efficient care for patients. A recent article in Healthcare IT News captured this challenge stating that 'healthcare requires an informed balance between delivering care and protecting patient information.'

   That is best achieved when both IT and information security staff have a close working knowledge of how the caregivers are using IT and information to get the mission done.' When accounts are not managed or governed properly, as noted in the Annals of Internal Medicine study, and do not balance organizational security with user efficiency, they can be more easily compromised and potentially lead to an increase in costly data breaches for the health system. In fact, according to the 2019 Cost of a Data Breach Report by the Ponemon Institute, data breaches across healthcare organizations cost more than $6.45 million on average, higher than any other industry.

   Healthcare systems must also protect against medical device hijacking and ransomware attacks, where machines essential to providing quality care like imaging, implantable devices, and life-support devices have malware planted. Once installed, this malware can then move throughout the network to infect other devices, applications, and even the entire system.

   Most concerning, these attacks can cause medical devices to malfunction—putting lives at risk. Protecting against device hijacking and data breaches should be top of mind for healthcare organizations. Identity governance enables organizations to address the access challenges associated with these risks by intelligently managing user accounts and ensuring the right people have the right access to the right systems.

Pro Tip

The Importance of Penetration Testing and Network Threat Detection

Healthcare organizations are primary targets for attacks with the amount of sensitive data they protect. Leading healthcare organizations today regularly conduct **penetration testing** to increase visibility into the effectiveness of their defenses and reveal their most pressing risks, and then work to actively address those challenges. They also actively monitor their networks with **network threat detection** to ensure that alerts received are for verified attacks, especially on devices so critical for patient care.

2. **Increasing Regulatory Compliance:** With pressure to ensure that sensitive health information is protected, healthcare organizations are required to comply with the Health Insurance Portability and Accountability Act (HIPAA), and regularly prepare for audits. Compliance today is not only more challenging and complex, but also more important than ever before. It requires that healthcare organizations collect information related to data access controls, methods of monitoring activity related to electronic personal health information, integrity monitoring, authentication, and transmission security. Without the proper identity governance and administration tools, HIPAA reporting becomes a tremendous burden.

   But it's not just HIPAA compliance that has increased pressure on healthcare systems. A recent article in Becker's Hospital Review indicated that 'healthcare leaders are further burdened to comply with a variety of newly revised standards…including Centers for Medicare and Medicaid Services (CMS) and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO).' These increasing standards have become more complex and more strictly enforced, creating additional costs and demands on healthcare organizations that can detract from the focus on overall organizational security. This reinforces the need for healthcare organizations to leverage more effective and efficient security controls and systems to meet these increasing regulatory demands.

3. **Expanding Digital Adoption:** When the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted more than a decade ago, according to the CDC, it proposed 'the meaningful use of electronic health records throughout the United States healthcare delivery system as a critical national goal.' With monetary incentives to adopt EHRs, healthcare organizations have spent the last 10 years capturing patient data electronically, providing patients with electronic health information, increasing health information exchange between providers, and reporting on their participation.

   However, the threat of federal fines from data breaches and the potential for civil actions at the state level has added to the frustration and complexity healthcare providers encounter for digital adoption across their organizations. In fact, according to a survey of top healthcare executives in 2019, the digital healthcare organization was in the top five challenges healthcare organizations face today, according to Becker's Hospital Review. Since many organizations have now implemented EHR systems, it is critical that they actively evaluate user access to the sensitive information contained in these electronic systems.

Patients expect transparency, efficiency, and privacy during their healthcare experiences, requiring healthcare staff and caregivers to have the right access to deliver a high quality of care.

4. **Rising Costs to Deliver Quality Patient Care:** The cost to provide quality care to patients will continue to rise for healthcare providers. According to data from CMS examining national healthcare expenditures, overall health spending is 'projected to grow at an average rate of 5.5 percent per year between 2018 and 2027, and to reach nearly $6.0 trillion by 2027,' while prices for 'healthcare goods and services are projected to grow by 2.5 percent.'

   Healthcare organizations will continue to face increasing costs and the overall industry will see increased spending to deliver critical healthcare services to patients. This means that health organizations must increase efficiencies in all areas, ensure that staff can seamlessly access data and systems to streamline patient care, and become more selective and efficient in their use of access security technologies.

5. **Growing Patient-Consumer Expectations:** Understanding patient satisfaction has become a key metric for healthcare organizations. The shift toward patientcentered care has risen in importance for health systems as individuals have taken a more active role in advocating for their healthcare treatments and interactions. Patients expect transparency, efficiency, and Patients expect transparency, efficiency, and privacy during their healthcare experiences, requiring healthcare staff and caregivers to have the right access to deliver a high quality of care. privacy during their healthcare experiences, requiring healthcare staff and caregivers to have the right access to deliver a high quality of care. Growing patient expectations and public accountability will continue to place pressures on healthcare organizations to increase the quality and efficiency of care, and to ensure sensitive information remains secure.

   For example, the Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) survey has increased in importance during the last two decades, measuring patient perspectives in relation to their hospital experiences. This publicly reported survey enables patients to act more as consumers, identifying where they do and don't seek care. And according to HealthCatalyst, many healthcare providers will need to change their approach, 'especially as patients begin to shop for healthcare the way they shop for cars or electrician services—by searching the Internet, looking for quality metrics and patient reviews, and comparing prices.' With so much expectation and scrutiny placed on healthcare organizations today, ensuring a frictionless process for delivering care is essential—and that requires the right identity governance programs to support these processes.

Overarching challenges in the healthcare industry create significant roadblocks for healthcare organizations today and contribute to the need for establishing strong identity governance programs that keep health systems safe and ensure patients receive the quality of care they deserve.

6. **Increasing Merger and Acquisition Activity:** Within the healthcare industry, health systems continue to see increasing M&A activity, particularly among the largest healthcare organizations in the country. According to the latest KauffmanHall M&A Activity Report, 'total transacted revenue for Q2 2019 was $11.3 billion,' which was significantly higher than normal revenue transactions, and second only to the 2017 activity of $12.6 billion.

   This increase is based on the large amount of megamergers and mergers between hospitals and health systems nationwide, with 46 total transactions announced to date in 2019, according to the same KauffmanHall Report. And this activity is projected to continue, according to Modern Healthcare, further adding to the complexity of the healthcare landscape. With the healthcare organization constantly changing and the number of users and requirements to access multiple systems and resources across a health system continuously evolving, it is virtually impossible to manage this fluctuation without the right identity governance tools and programs in place.

7. **Growing Shortage of Qualified Talent:** The healthcare industry is expected to add more jobs than any other industry by 2022, according to the Bureau of Labor Statistics, with projections of nearly four million workers added since 2012. It's one of the fastest growing industries nationwide, but as Becker's Hospital Review indicates, healthcare doesn't have 'enough skilled people entering the workforce to fill the gap.' And that can translate into negative consequences for quality and efficiency of care.

   Beyond skilled healthcare workers, finding qualified talent for IT and security within healthcare organizations is also a significant challenge. According to CIO, 'health IT shortages are substantial and growing,' and 'tens of thousands of jobs are needed to meet growing IT demands within healthcare organizations.' Health systems must find the right IT talent who can keep up with increasing regulations and who can do more with less to effectively manage user access across the organization.

8. **The Contingent, Mobile Healthcare Workforce:** Many healthcare organizations today have started relying on a contingent workforce in response to overall workforce shortages and to address the rising costs of hiring full-time healthcare employees. These contracted employees often are hired for a short-term period or on-demand basis, and are continuing to increase across the healthcare sector. In fact, the American Staffing Association estimates that throughout the United States, nearly 1.6 million temporary and contract employees now work in the healthcare industry. This reliance on contract or contingent employees creates a highly mobile workforce, where new healthcare professionals are continuously rotating across the expansive networks of healthcare offices and systems, creating increased security risks and demands for intelligent access management across health systems today.

These overarching challenges in the industry create significant roadblocks for healthcare organizations today. And together, they contribute to the need for establishing strong identity governance programs that help keep patient and healthcare system information safe and ensure patients receive the quality of care they expect. With these primary challenges in mind, let's now take a look at the top five drivers of identity governance for the healthcare sector to more clearly understand how intelligent identity governance can address these challenges.

Top Five Drivers of Identity Governance and Administration in Healthcare

Healthcare organizations seeking to address the major challenges in their industry turn toward identity governance and administration programs to more intelligently and effectively address identity and access management in their organizations. Figure 1 represents the top five organizational drivers for healthcare systems today and their needs for strong identity governance, including regulatory compliance, risk management, external pressures from organizational change, managing costs and driving value-based care, and improving IT service delivery.

Figure 1: The top five drivers for identity governance and administration in healthcare organizations today.

Healthcare organizations seeking to address the major challenges in their industry turn toward identity governance and administration programs to more intelligently and effectively address identity and access management in their organizations.

Healthcare organizations leverage Identity Governance and Administration solutions to demonstrate their compliance with industry mandates and more easily respond to audit demands. To manage risk more effectively, healthcare security professionals can use IGA to enforce security policies, protect sensitive data from unauthorized access, eliminate excess privileges, terminate orphaned accounts, and uncover segregation of duty violations within the healthcare system.

In order to respond to continuous organizational change within the healthcare sector, healthcare providers can look to IGA solutions to manage access-related activity for mergers and acquisitions, health system reorganizations, seasonal staffing changes, ongoing healthcare employee changes or transfers, and to oversee provisioning for the contingent workforce.

Identity governance programs also enable healthcare organizations to ensure the right access is given to the right people at the right time, reduce reliance on helpdesk support, and decrease audit-related costs for healthcare teams. Finally, healthcare leaders seeking to improve IT service delivery can rely on IGA to onboard new hires faster, reduce administrative burden for managers, and streamline overall health system identity governance processes—enabling the organization to do more with less.

Critical Healthcare Identity Governance Challenges

Responding to the most pressing issues in the healthcare industry, and the top drivers for effective identity governance and administration, healthcare organizations have specific identity governance challenges they must solve to make their organizations more secure in the face of ongoing change. Manual provisioning processes, insufficient visibility into existing account access, and the lack of automation significantly contribute to these challenges, magnifying the time and resources required to oversee and manage user access.

Because many healthcare organizations still lack a centralized process to manage and audit user accounts, they often have very little visibility into the actual access levels users possess. According to a recent study by Cybersecurity Insiders, only 53 percent of organizations today are confident in the effectiveness of their identity and access management programs. This translates directly to the challenges healthcare organizations face. With only half of all organizations today confident in their IGA programs, healthcare providers face an upward climb to ensure their identity and access management is effective across their environments. Here are some of the top access-related challenges that health systems encounter today:

1. **Effectively creating and maintaining access for a diverse, mobile, contingent, and rotating workforce:** With varying levels of access required for multiple user types, including employees, clinical staff, medical students, interns, and non-employee clinicians, healthcare security professionals must ensure they intelligently create, monitor, manage, and remove access in a timely manner for employee and non-employee user accounts. This also means securely and efficiently enabling appropriate levels of access across an expansive network of health systems to enable users to effectively perform their jobs.

Because many healthcare organizations still lack a centralized process to manage and audit user accounts, they often have very little visibility into the actual access levels users possess.

2. **Addressing the ongoing complexity and granularity of user roles across titles, departments, and applications:** In addition to managing a mobile, diverse workforce, healthcare organizations must oversee a complex network of health system applications and devices, and ensure their identity governance programs address the specialization and granularity of user roles across departments, titles, and user types. Health systems should operate with the policy of least privilege, while still providing users enough access to effectively perform their critical roles within the healthcare environment.

3. **Increasing time and resource requirements for provisioning:** The complexity and changing nature of the healthcare workforce has contributed significantly to the time and resources required for user provisioning within health systems today. These growing demands continue to put strain on IT healthcare teams to keep up with provisioning and deprovisioning accounts, and ensuring appropriate levels of access are given to the right users.

4. **Ensuring patient privacy and frictionless access to personal health information:** With increasing industry and government mandates around electronic health records and patient data, health organizations must ensure they are continuously storing health information securely to meet regulatory compliance. This includes monitoring and prioritizing access risks, giving appropriate access levels to healthcare staff and patients, and uncovering hidden access levels within the organization. Healthcare organizations must also practice the policy of least privilege access so only those users that need access to patient data receive it the moment they need it.

5. **Managing brand reputation, access risks, and trust:** Healthcare organizations today know the value of keeping personal health information secure. And they also know the high cost that a data breach can have on their organization—both in terms of monetary costs and loss of brand reputation. Ensuring patients and users can trust the organization to keep health information secure and have solid, reliable identity governance programs to keep sensitive data safe is essential for healthcare organizations today.

The reality is that with so many systems and so many access privileges to manage, it is extremely difficult for healthcare organizations to understand what access employees and non-employees need, and then control that access without the right identity governance programs. Research from Cybersecurity Insiders also describes the complexity of access challenges today and the risk this presents to an organization. According to its 2019 Identity and Access Management Report, more than 70 percent of users have more access privileges than required for their job. When healthcare users have more access than they need, there is an increased opportunity to target users with elevated access levels resulting in increased risk. And the problem only magnifies with contingent workers or accounts that are orphaned. This risk becomes even greater if excess privileges are unused because nefarious access can go undetected. Combined together, these factors make it very difficult to limit risk within the business, especially, as in healthcare, high numbers of employees and non-employees join or leave the organization.

Strategies for Leveraging an Intelligent, Effective IGA Program within Healthcare Organizations

The challenges that healthcare organizations face in relation to protecting sensitive data and ensuring the right people have the right access to the right systems at the right time may seem overwhelming. But with the right strategies to guide their organization, healthcare providers can leverage a best practice approach for identity governance. The following six strategies provide a framework for healthcare organizations to improve the quality and efficiency of their identity governance and administration programs, ensuring healthcare data security, protecting sensitive assets, and supporting ongoing compliance, so they can focus on what matters most—their patients.

Strategy 1: Automate Account Provisioning and User Lifecycle Management for Healthcare Technology Systems, Platforms, and Applications

The first strategy for establishing an effective identity governance program is to automate provisioning around a user's lifecycle within the organization. This can start with the user's first relationship with the health system as a job applicant, contingent worker, or employee, and conclude with the user separating from the organization. In between these events are multiple changes, and access requirements that must be closely managed. Within the user lifecycle, onboarding is typically the first step, where a new healthcare employee or contingent worker receives initial accounts and access to the appropriate systems and applications.

Figure 2: The basic stages of the user lifecycle.

Once onboarded, a user may need new or different access, particularly when transferred within the health system. This occurs when a healthcare professional changes job roles or needs to perform different duties within a separate department or location—even temporarily. It can also include transfers to a new department or reporting to a new manager. The last stage occurs when a worker leaves the organization, either voluntarily or involuntary. For the latter, accounts should be quickly and automatically disabled, preventing any opportunity for the user to retain access to healthcare data or credentials upon their departure.

Automating provisioning around the user lifecycle truly enables caregivers and staff to be productive on day one rather than waiting around for access within the health system. It also decreases the reliance on IT resources, while improving security by reducing the risk that access will be 'borrowed' during this period and decreasing the risk associated with manual provisioning and deprovisioning mistakes. At the very least, when provisioning automation is not practical or feasible, automated workflow and access policies for requesting, approving, tracking, and auditing should be deployed. Healthcare organizations that automate provisioning around the user lifecycle should ensure this part of their identity program enables them to:

- ✓ *Create base access for new users from an authoritative source*
- ✓ *Remove user access based on direction from authoritative source*
- ✓ *Empower manager requests for user access*
- ✓ *Accommodate contingent workers, like non-employee clinicians, based on manager direction*

Check out Core Provisioning later in this guide to learn how you can easily automate access requests and account creation in your organization.

Strategy 2: Visualize Relationships Between Users and Access within the Complex Healthcare Structure

For healthcare organizations to understand the right levels of access to assign, what to change those levels of access to when necessary, and what to review them against, they should adopt a role-based approach that leverages role-based policies. As defined earlier in this guide, think of a role as a collection of access privileges typically around a job title or job function. Using roles, healthcare organizations can establish solid, predefined, and preapproved access policies and know specifically which access privileges each person needs.

This strategy simplifies identity governance and administration, and aids healthcare organizations particularly as they grow and change. Embracing a role-based approach also decreases the timeline in executing bulk additions where a lot of change is happening at once, like during mergers and acquisitions, fluctuations in healthcare staffing, and reorganizations. This strategy also works well to improve the efficiency of staffing assignments in high turnover areas or highly competitive talent areas like nursing.

Using an industry-leading role designing tool with cluster analysis and a 'visual-first' approach to group like-access privileges together, healthcare organizations can better understand the access that individuals have in common and what outliers might be present, rather than trying to use a spreadsheet to make sense of the data. Healthcare organizations that want more intelligent and visible identity governance across all of their environments should consider a visual-first approach that enables them to:

- ✓ *Easily view role definitions across multiple user types*
- ✓ *Gain insight into user access across the organization*
- ✓ *Determine whether overprovisioning or underprovisioning is occurring*
- ✓ *Identify whether similar users are receiving the right roles*

Check out Core Role Designer later in this guide to learn how you can accurately visualize relationships between users and access levels within your healthcare organization.

Strategy 3: Streamline Access Requests and Approvals to Increase Security and Efficiency Across the Healthcare System

For healthcare organizations to be successful in establishing effective identity governance programs, they need to leverage a one-stop shop for user access. This strategy prescribes that healthcare providers deploy one centralized portal to complete access requests and approvals. Providing a central hub for users to request additional access ensures healthcare employees and contingent staff go through the proper channels for access to the expansive network of health system applications and platforms, and makes certain that proper approval and fulfillment policies are followed. Leveraging a centralized system makes it easy for users to request access, but it also provides a consistent method for creating accounts and entitlements consistent with healthcare policies and protocol. Health systems that streamline access requests should ensure this portion of their identity program includes:

- ✓ *A central platform for access requests and approvals*
- ✓ *The ability to streamline employee or contingent onboarding*
- ✓ *Automation to remove employees or non-employees who leave the organization*
- ✓ *Functionality for integrated role management*

Check out Core Access later in this guide to learn how you can streamline access requests and approvals in your organization.

Pro Tip

Leverage a centralized portal for user access requests and approvals.

Strategy 4: Simplify the Access Review Process and Respond to Ongoing Healthcare Compliance Demands

Health systems that view regulatory compliance through the lens of an IGA program recognize they should monitor access continuously and provide access to only those individuals that need it, enabling the organization to stay more compliant. IGA solutions not only ensure access to information like patient records or financial data is strictly controlled, but also enable healthcare organizations to prove they are taking actions to meet compliance requirements. Conducting frequent access reviews or certifications is a key area for enhancing identity governance.

Within the climate of regulatory compliance, especially increasing auditor demands around HIPAA, it is imperative for healthcare organizations to review user access periodically. Access reviews must be simple and easy, so managers do not just instantly grant approval.

While many healthcare systems use a manual process, passing around spreadsheets among reviewers, a more intelligent, visual approach is a must-have to start grouping like-access privileges together. This enables managers across healthcare organizations to understand which users—whether employee or non-employee—have access to specific systems, and which users are outliers in their privileges. Leveraging an easier review process leads to greater accuracy, improved reporting, and greater adoption within the organization.

Another key element for healthcare organizations to consider as part of their review process and broader IGA program is micro-certifications. Since the time between new provisioning and the next audit or review process can be fairly lengthy, it is important to have a set of controls that can quickly identify anomalous access, especially when that access violates an important policy, such as segregation of duties or privileged access. This can be done through the use of micro-certifications.

Micro-certifications allow managers within the health system to be alerted when an employee may have new or updated access and entitlements other than what is expected, or if staff gain access through an outside process, commonly referred to as out of band. This alert allows the approver to perform an immediate access review associated with the event, significantly reducing any chance of insider threats within the system, enabling the organization to meet ongoing regulatory compliance, and allowing for any exceptions that might be necessary. Health systems seeking to streamline the access review process should ensure an automated certification process empowers them to:

- ✓ *Easily identify and manage access rights for applications*
- ✓ *Conduct access certifications to applications and file shares*
- ✓ *Remediate inappropriate or high-risk access*
- ✓ *Respond to compliance audit demands*

Check out Core Compliance later in this guide to learn how your organization can automate access certifications in your organization.

Pro Tip

Take advantage of automated micro-certifications to ensure any new or revised access or entitlements can be reviewed immediately.

Strategy 5: Enforce Strong Password Management Across the Healthcare Organization

With so many systems, applications, and users, it can be difficult for healthcare organizations to ensure employees and contingent workers are regularly changing their passwords, so it is important to have frequent mandatory password resets. It is also important to maintain password policies that enforce complexity and non-reuse rules. However, the problem with password resets is that users may forget their newly updated passwords, requiring additional IT resources to support a simple reset—taking valuable time away from focusing on more strategic initiatives. One way to combat this challenge is to leverage a strong self-service password solution that enables healthcare professionals to securely reset their own passwords.

Leading password reset solutions allow users to also unlock their accounts through self-service mechanisms. A variety of password reset options, such as a mobile reset application or telephonebased keypad resets, Windows Credential Provider and voice biometrics help increase user adoption rates, while maintaining a secure reset channel. Healthcare organizations seeking to improve the strength of their overall identity governance program should enforce strong password management across the organization and look for a solution that:

- ✓ *Delivers faster, more convenient user self-service*
- ✓ *Synchronizes passwords on multiple systems*
- ✓ *Reinforces strong password policies*
- ✓ *Reduces password-related help desk calls*

Check out Core Password later in this guide to learn how your healthcare organization can empower users with a self-service password solution.

Pro Tip

Empower users to leverage self-service mechanisms for password resets, like SMS, mobile app, or telephone.

Strategy 6: Reduce Certification Fatigue and Increase User Adoption within the Healthcare Organization

Reviewing entitlements without adequate user context is overwhelming within the expansive network of a healthcare system. Yet this is a common practice and can lead to inaccuracies and excessive distribution of access, particularly among a contingent workforce. Underprovisioning healthcare professionals can also lead to increased risk and lack of productivity if credential sharing occurs or specific users do not have the right access to do their jobs. For healthcare organizations to build a more effective identity governance program, they must empower managers and approvers to simplify the review process.

And one of the best strategies to do this is through streamlined visualization of common user entitlements. This enables reviewers to quickly and easily compare access to others, adding essential context during the review process. Increasing operational efficiency also results in higher user adoption rates across the healthcare organization—and that goes hand-in-hand with increasing overall security posture. Healthcare organizations that make it part of their overall strategy to reduce certification fatigue through a more contextual and visual solution solve the essential challenges related to:

- ✓ *Requiring approvers to conduct too many certifications*
- ✓ *Manually certifying user access across multiple user types*
- ✓ *Providing insufficient contextual information about user access*

Check out Core Certify later in this guide to learn how your healthcare system can reduce certification fatigue and create a visual approach to access certifications.

Pro Tip

Add context to access reviews and certifications by leveraging a visual-first approach that compares access between users.

Leading-Edge Identity and Governance Administration Solutions for Healthcare Organizations

Healthcare organizations have unique needs and requirements when it comes to identity governance. And Core Security understands this. Healthcare systems require intelligent solutions to address their expansive networks, systems, and applications. They need to automate provisioning across a disparate workforce. And they need to secure critical healthcare data and information, while demonstrating ongoing regulatory compliance.

Core Security is a leading provider of Identity Governance and Administration solutions to the healthcare industry. Our solutions streamline access management, reduce the overall threat surface, decrease IT costs, and support compliance for health systems of all sizes. The Core Security solution portfolio includes two leading-edge suites that have been recognized by industry analysts, including Gartner.

How Core Security Offers Leading-Edge Identity Governance and Administration Solutions

Core Security provides intelligent and visible Identity Governance and Administration solutions to organizations across the healthcare sector, enabling them to improve security, boost efficiencies, and ensure ongoing compliance. Here's a glimpse at how our portfolio of award-winning IGA solutions make an impact for healthcare today:

- Improve quality of service and patient care by ensuring healthcare professionals have the right access to the right systems, applications, and resources at the right time
- Enable effective rollout and expansion of EHR solutions and meaningful use programs by providing seamless user and patient access to all relevant applications and data
- Avoid potential audit findings from HIPAA and other mandates by adopting tools to detect and correct inappropriate access and behavior
- Leverage our depth of expertise in the healthcare market to ensure program success without diverting resources from patient care or securing patient information
- Adopt a phased implementation approach that enables healthcare organizations to realize identity governance solution benefits quickly

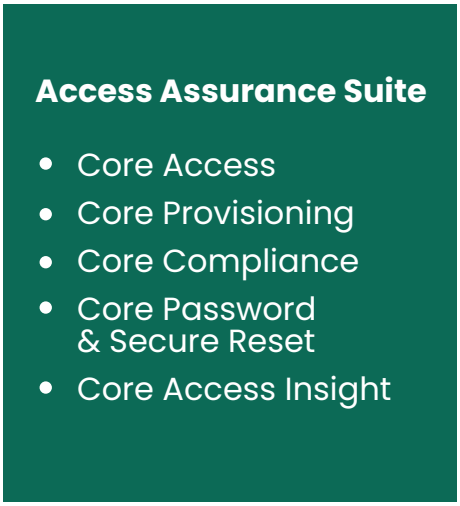


Figure 3: Award-winning solution components of the Core Security IGA Portfolio

Core Security Solution Portfolio

Access Assurance Suite

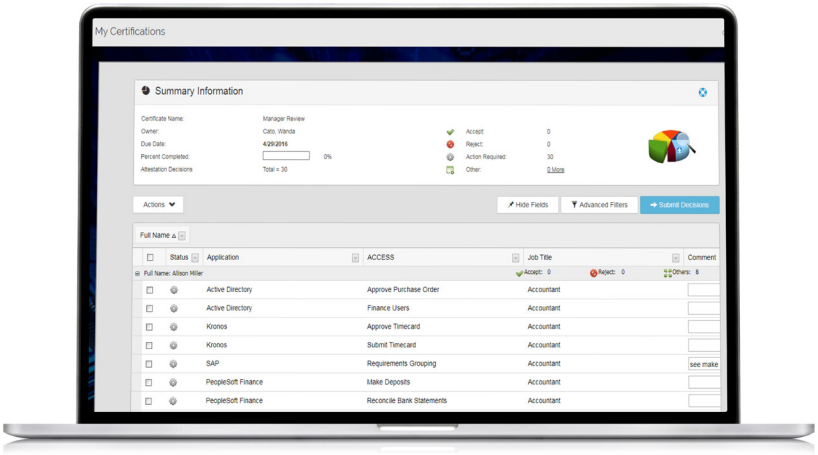
An integrated Identity Governance Solution that delivers informed provisioning, continuous compliance, and actionable analytics. Comprised of four industry-leading modules, the Access Assurance Suite enables healthcare organizations to streamline the provisioning process, review access requests, easily manage compliance, and enforce robust password management in one complete solution.

- **Core Access:** A convenient web portal where end users can request access and managers can review, approve, or deny access. Using a shopping cart approach, Core Access delivers an efficient and user-friendly experience—replacing paper forms, emails, and tickets used to manage access. Plus the ability to leverage roles enables access to be assigned quickly and accurately.

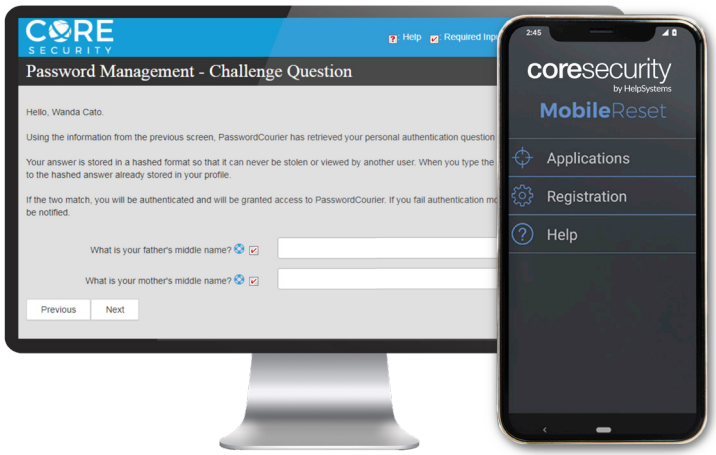
- **Core Provisioning:** As the backend fulfillment engine for Core Access, Core Provisioning uses software connectors to programmatically create and manage user accounts based on policies and permissions set up in Core Access. Our solution offers automated provisioning actions on hundreds of applications used across industries, organizations, and departments.

The Access Assurance Suite is a good choice for organizations that require a balanced approach to provisioning and access governance, with built in support for analytics.

Gartner Critical Capabilities for Identity Governance and Administration



- **Core Compliance:** Identify and manage access rights for systems, platforms, and applications in a single interface, eliminating the need to review spreadsheet after spreadsheet. Immediately respond to compliance audit demands to ensure adherence to regulations like SOX, HIPAA, PCIDSS, and GDPR.



- **Core Password and Secure Reset:** Core Security provides a complete, integrated solution for automated password management. Core Password and Secure Reset work together to provide a convenient and secure password reset solution for your organization. Leverage simple, secure selfservice password resets to automate password management and reduce access risks. Easily enforce robust password policies and empower users to streamline security in your organization.

Core Access Insight

Access Insight offers a continuous, comprehensive view and analysis of the relationship between identities, access rights, policies, and resources that occur across your entire environment. Our easy-to-use solution applies analytics to the big identity and access data in your organization, empowering you to identify risks, and drive provisioning and governance controls to manage that risk within your business.

- *Evaluate and act upon risks associated with user access and activities*
- *Easily identify and remediate improper user access that could harm your organization*
- *Analyze massive amounts of identity and access data against policies*
- *Make informed decisions about the appropriate access designated to each role in your organization*
- *Understand complex access structures through intuitive visualizations*

Access Insight works with the industry-leading portfolio of solutions from Core Security, or in conjunction with other IGA solutions, to identify potential risks to the business, so you have a continuous and comprehensive view of your network and can quickly modify access as needed.

Intelligent Identity Governance in Action

When a not-for-profit healthcare organization with more than 350 employee physicians and 400 non-employee affiliated physicians, across more than 50 clinical applications, recognized the limitations of its manual identity governance processes, it selected Core Security Identity Governance and Administration solutions to automate user provisioning, account disabling, self-service password management, and access verification. The organization implemented an automated solution that would increase the reliability of user IDs and passwords, maintain the integrity of information that was becoming unmanageable, and support a critical mass of healthcare users and applications.

Since implementing Core Security solutions, the health organization has enforced a strong password management policy that eliminates loopholes and errors in the password reset process. It has also adopted a role-based approach to access control and has plans to implement roles for employees, credentialed doctors, nurses, and departmental staff, ensuring access rights will be linked to roles within the organization. By automating its provisioning process, the organization has also reduced time to access from months to just minutes. Since deploying Core Security IGA solutions, the not-for-profit health organization has achieved a more productive, efficient approach to managing identities, avoiding the costs associated with hiring additional staff, demonstrating regulatory compliance by enforcing strong security policies, and streamlining access control and the auditing process.

Start Your Journey to Intelligent and Visible Identity Governance and Administration with Core Security

There is too much at stake for healthcare organizations today to ignore the importance of implementing a strategic, intelligent identity governance program. Investing in leading IGA solutions from Core Security enables health organizations to significantly decrease their risk of attack, supports streamlined regulatory certification and compliance, and increases operational efficiencies—keeping valuable personal health information safe and keeping healthcare professionals focused on providing quality care to patients.

Ready for IGA programs that protect your organization in the face of change?
Get a live demo of Core Security Identity Governance and Administration solutions from one of our experts today.
www.coresecurity.com

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.