FORTRA

Wellspan Health

Identity Governance Administration Case Study

Background

Serving south central Pennsylvania and Northern Maryland, WellSpan is a not for-profit community resource that provides more than $18 million each year in uncompensated medical and outreach services, supplies and physician care.

The Challenge

Through its acquisition of medical offices and health centers, WellSpan has experienced significant growth, leading to a substantial increase in the number of clinical applications and users it supports. With more than 50 different clinical applications running across the organization and a user population that includes 300- 350 employee physicians and 350-400 non-employee affiliated physicians, WellSpan recognized that it needed to make changes to its manual operations and pursue the implementation of automated identity management and user provisioning in order to provide the best employee experience and deliver superior patient care.

In its pursuit of an automated solution to address its identity management and user provisioning challenges, WellSpan identified the following key objectives in its effort to improve employee access and productivity while demonstrating the necessary security and regulatory compliance:

+ Automating the provisioning process to grant employees access to the appropriate patient information to streamline patient care

+ Implementing self-service password management

+ Verifying access control

+ Demonstrating HIPAA and other regulatory compliance

WellSpan used these objectives as a guideline for identifying the solution to meet its automation, security, and regulatory needs.

OVERVIEW

WellSpan selected Core Security's Identity Governance Administration Solution to ensure that access to information, buildings and systems were given to the right people at the right time. Key results include:

+ Increased operational efficiency and transparency

+ Strengthened security

+ Improved compliance

+ Delivering fast time to value and the lowest total cost of ownership

> *"By automating the provisioning process, WellSpan was able to drastically reduce time to access from months to mere minutes. The time and cost savings of provisioning 40-60 new hires and de-provisioning ten to 20 terminations per week are more than significant."*
>
> **- William Gillespie, VP and CIO, WellSpan Health**

The Approach

WellSpan chose the Core Security's Identity Governance Administration solution to automate user provisioning, account disabling, self-service password management and access verification. WellSpan selected Core Security because of the company's proven ability to streamline the user provisioning process while providing the foundation for a strong identity management security policy and ensuring adherence to compliance requirements. Additionally, Core Security had the only solution that demonstrated it could easily integrate with the hundreds of healthcare-specific platforms currently deployed such as Cerner Millennium, Eclipsys, and GE Healthcare Centricity RIS-PACS.

In advance of kicking off its automated user provisioning, WellSpan created a comprehensive Electronic Health Record (EHR) for every patient. While centralizing all patient data in one record improved efficiency for administrators and clinicians, WellSpan recognized that EHRs presented privacy and security challenges. WellSpan needed to ensure that access to health information was controlled without disrupting the clinical workflow, while at the same time ensuring that audit and compliance requirements are being met. The Core Security's Identity Governance Administration solution demonstrated the ability to grant the appropriate user access to EHRs in the clinical systems, while doing it in compliance with government regulations for patient privacy.

Managing the Identity Crisis

A common challenge among healthcare organizations is to ensure that users have proper access to clinical applications and patient data so they can deliver effective patient care. Additionally, this access must be granted in compliance with government regulations requiring minimum necessary access and patient privacy. WellSpan's challenge was no different – the need to provide its clinical workforce appropriate access to vital patient information through a variety of clinical systems to effectively and immediately provide patient care.

To manage the identity crisis resulting from granting application access, resetting passwords and adhering to compliance requirements, WellSpan decided to implement 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 users and applications.

Automated user provisioning and self-service password reset immediately improved WellSpan's productivity, while still enabling WellSpan to maintain tight control over access to its clinical systems. Even while computer terminals we being shared by multiple employees, contractors, and additional third parties, WellSpan adhered to HIPAA regulations and its own security and compliance standards.

Moving from Manual to Automated Processes

In choosing an automated provisioning solution, WellSpan needed to address four main areas: supporting merger and acquisition activity and continued growth in clinical applications and IT users; streamlining access changes which were taking up to three months; demonstrating HIPAA and other regulatory compliance; and enabling care transformation by facilitating clinical application access control.

With a deep penetration in the healthcare market and a history of successful customers in production, Core Security's Identity Governance Administration solution demonstrated the ability to streamline the user provisioning process while providing the foundation for enforcing security policies and ensuring adherence to compliance requirements.