Case study: Enhancing identity and access governance in health care with RAC/M Identity

OKIOK

RAC/M IDENTITY

Context

Our client, a major university teaching center in Montréal, is one of the region's leading healthcare institutions, offering a full range of medical services to the population.

With several tens of thousands of identities to manage, high organizational complexity due to the large number of healthcare institutions, hospitals, clinics and other entities, the Center faced significant identity governance challenges.

Challenges

High volume of diversified identities

The Center needs to manage several tens of thousands of identities, such as employees, doctors, patients, suppliers, researchers, guests, students, trainees, and residents.

Organizational complexity

As a university teaching center, the Center is made up of many healthcare institutions, hospitals, clinics, and other entities, resulting in high organizational complexity.

Access rights management

Managing access rights and authorizations in such a vast and diverse environment is a major challenge, requiring a strategic approach and appropriate tools.

Regulatory compliance

As a healthcare establishment, the Center must comply with the requirements of the Québec Ministère de la Cybersécurité et du Numérique (MCN), the directives of the Québec Ministère de la Santé et des Services Sociaux (MSSS), as well as cybersecurity and personal data protection regulations, which requires effective governance of identities and accesses.

Complexity and volatility of the user population

Interns and university residents make up a significant proportion of the Center's user population. They must be granted appropriate access quickly at the start of their internship, and this access must be revoked promptly at the end of the internship.

The creation, modification and deactivation of trainee and resident accounts and accesses generates a very high volume of manual operations, representing a huge manual workload. This entails significant costs, delays and risks of error.

Imminent move to a super hospital

The Center planned to move into a new state-of-the-art super hospital where physical access to all areas and thousands of doors and rooms would be strictly controlled, adding another level of complexity to access management.

The solution: RAC/M Identity™

To meet these challenges, the Center chose to implement the RAC/M Identity governance and administration (IGA) solution. This solution streamlines identity and access management, enhances data security and improves regulatory compliance.

Integration of multiple identity sources

The RAC/M Identity solution successfully integrated with the Center's multiple identity sources, enabling centralized, unified identity and access management across the organization, simplifying processes, and improving data consistency.

Self-service portal integration

The RAC/M Identity solution has been integrated with the Center's self-service portal, enabling managers and super-users to manage the creation of new identities and request access autonomously, thus reducing the workload on IT teams.

Integration into the university resident process

The RAC/M Identity solution has been integrated into the university resident management process, by which universities produce lists of residents, including the departments and services in which residents will be doing their internship, as well as start and end dates.

From these lists, the RAC/M Identity solution automatically creates accounts and grants the required access to the relevant systems and applications. At the end of the course, accesses are withdrawn, and accounts deactivated.

Integration with physical access systems

In addition, RAC/M Identity was integrated with the Center's physical access systems to generate and manage access cards. This integration has automated the process of issuing and managing access cards, improving the user experience, operational efficiency, and security by reducing delays and manual operations.

Integration into the technological environment

The flexibility of the RAC/M Identity solution made it possible to integrate a very large number of systems and business applications. For example, RAC/M Identity ensures

that passwords are propagated to systems and applications when a password is changed in the AD directory.

Results

Streamlining identity management

The RAC/M Identity solution has helped simplify and streamline identity management in a complex and diverse environment, improving operational efficiency.

In fact, the implementation of a perfectly synchronized repository with multiple identity sources has substantially reduced software licensing costs, helping to finance part of the RAC/M Identity solution.

Enhanced data security

By automating the arrival/departure circuits for trainees and residents, and applying an access model based on RBAC roles, the Center has strengthened data security and confidentiality, and aligned its practices with industry best practice.

Enhanced regulatory compliance

The RAC/M Identity solution has enabled the Center to better meet MCN regulatory requirements and MSSS guidelines for data security and confidentiality, thus reducing the risk of non-compliance.

Improving operational efficiency

Integration with the self-service portal and physical access systems has improved operational efficiency and reduced the costs, delays and errors associated with manual identity management.

Conclusion

The collaboration between the Center and OKIOK in implementing the RAC/M Identity solution has significantly enhanced identity and access governance.

By adopting a strategic approach and implementing advanced identity and access management tools, the Center has strengthened its data security, improved regulatory compliance, and optimized its operations.

To find out more about RAC/M Identity and how it can benefit your organization, please visit our website at www.okiok.com or contact our sales team at sales@okiok.com.