CASE STUDY: Children's National Medical Center - Automating User Access Rights Compliance with Access Auditor®

Background

Children's National Medical Center (CNMC) is the only exclusive provider of pediatric care in the metropolitan Washington, DC area and is the only freestanding children's hospital between Philadelphia, Pittsburgh, Norfolk, and Atlanta. Serving the nation's children for more than 130 years, Children's National is a proven leader in the development and application of innovative new treatments for childhood illness and injury. Serving as an advocate for all children, Children's is the largest non-governmental provider of pediatric care in the District of Columbia, providing more than $50 million in uncompensated care. Children's National is proudly ranked consistently among the best pediatric hospitals in America by US News & World Report and the Leapfrog Group.

Children's National wanted to quickly improve their control and management of critical business applications. With over 6000 employees integrated throughout many core applications, the review and certification of user access rights was a highly labor-intensive manual process. After a rapid three day deployment, Access Auditor from Security Compliance Corporation (SCC) provided the hospital a central repository of user access rights. SCC's Identity Mapper™ consolidated identity information and immediately discovered orphaned user accounts left behind following employee terminations. In addition, Access Auditor's advanced rules-based workflow engine streamlined the access rights re-certification process and enabled the hospital to conduct role-based privilege reviews with much greater speed and accuracy.

The Challenge

As one of the nation's leading hospitals, Children's National is subject to the HIPAA privacy rules and maintains strict controls on protected health information (PHI). Auditing user access rights to the systems and applications that host this sensitive data is a key control and must be closely monitored. CNMC's Information Security team was performing regular reviews and audits of user access data, but without the proper tools, the effort was very time-consuming and inefficient. Each application was reviewed individually and spreadsheets of data were cross-referenced by hand in an attempt to detect user accounts left behind following an employee termination. Moreover, each review was a one-time event. Results could not be reused and the entire process was repeated with every review cycle.

The Challenge

CNMC needed to automate the certification of user access rights and the identification and removal of user accounts left behind from terminated users.

The Solution

Access Auditor automated the re-certification process and the Fuzzy ID Identity Mapper enabled the discovery and removal of orphaned user accounts.

The Results

Following a rapid 3-day deployment, CNMC established a consolidated repository of user access rights and enhanced their security and protection of sensitive health records.

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(866) 657-4550
www.securitycompliancecorp.com
info@securitycompliancecorp.com

"SCC's Identity Mapper with the Fuzzy ID module has allowed us to map user accounts from a wide variety of systems back to the same physical person, giving us a true consolidated view into user access rights. Access Auditor has automated our process of discovering and removing orphaned user accounts, and will help us streamline our periodic review and certification of user access rights."

Matthew Hicks, Director of Information Security

With over 6000 employees, reviewing user access rights would be a monumental task even under the best of conditions. Since Children's National faced common challenges such as limited resources and a lack of existing tools, the following requirements were identified for an access rights certification solution:

- Create a central repository of user access rights. Each system had its own unique data store and format for reporting, complicating the review process. Any solution should easily consolidate this data.
- Provide identity mapping without a unique login ID. Common in most companies, legacy applications evolve independently and often do not share a common login ID. At CNMC, no common user identifier existed across all applications, and occasionally names would be misspelled or more than one user would share the same name. The challenge of linking accounts from various systems was a critical requirement.
- Simple deployment and easy operation. As a non-profit institution, resources are efficiently allocated and large, expensive software tools must provide a clear return on investment. Large identity-management suites were therefore not a good fit. The hospital needed a simple and targeted solution.
- Provide a high level of automation. Each access rights certification was a repeat of the same manual process with no possibility for reusing results. Since no efficient way to delegate the certification authority to the various department heads existed, the security team bore the brunt of the entire attestation process. Any potential solution should automate the user access re-certification process.

In summary, Children's National faced many of the same challenges shared by thousands of companies today. User access rights are stored in independent applications without a central repository or a common unique identifier. Review and certification of access rights are very labor-intensive and companies need a simple and efficient automated solution.

The Solution

Franc Njoku, IT Security Auditor, and Matt Hicks, Director of Information Security, sought to automate their user access rights certification process. Access Auditor from Security Compliance Corporation provided the ideal solution. With its intuitive design and easy administration, Access Auditor was just what the doctor ordered for the hospital.

Working with SCC, Children's National identified the largest pain points and developed a simple plan to deploy Access Auditor. The first step was to import

data into a centralized repository. Without a common login ID, identifying the same person in multiple applications is an overwhelming task. However, thanks to Access Auditor's Identity Mapper, CNMC not only consolidated these accounts, but also populated Active Directory with data from the HR system of record.

"Like many organizations, we have a variety of systems and legacy applications with no common user identity key. SCC's Identity Mapper with the Fuzzy ID module has allowed us to map user accounts from a wide variety of systems back to the same physical person, giving us a true consolidated view into user access rights," said Hicks. "Access Auditor has automated our process of discovering and removing orphaned user accounts, and will help us streamline our periodic review and certification of user access rights."

After creating the centralized repository of access rights data, Access Auditor immediately began delivering results. With a single click, orphaned user accounts were instantly identified. Reports were readily available showing a consolidated view of who has access to what. What used to be a time-consuming, manual process was replaced with Access Auditor's automated imports. Account and privilege data was scheduled to be re-imported on a nightly basis, keeping Access Auditor's identity warehouse current and alerting to changes in sensitive privileges.

The entire process of installation, configuration, and importing of data into Access Auditor for 6000 users across five key applications was completed in three days.

The Results

Children's National Medical Center saw tremendous results. The Fuzzy ID Identity Mapper and bulk updating tool allowed CNMC to synchronize user accounts from disparate systems. The centralized repository of access rights provides real-time information about user roles and privileges, and instantly identifies any accounts left behind from terminated users.

In addition, the labor-intensive review and certification process was replaced with Access Auditor's role-based automation, resulting in a savings of countless staff hours. The hospital can now distribute the certification to department heads and other approvers without sending a myriad of spreadsheets. All of the approvers are notified by email, each performs the certification via a simple web page, and the full history and authoritative evidence of compliance are saved in one place for future reporting.

Michael Lavorel, Executive Director of Information Resources Technology, summarizes the benefits for CNMC. "Access Auditor allowed us to move away from a labor-intensive manual process to an automated process that has saved us many labor hours."

"Access Auditor allowed us to move away from a labor-intensive manual process to an automated process that has saved us many labor hours."

Michael Lavorel, Executive Director of Information Resources Technology

Access Auditor Key Features

FEATURE	DETAILS	BENEFITS
Entitlement Reviews and Access Certification	• Managers and business owners certify access rights with a simple web-based solution • Flexible rules-based workflow defines custom approvers at various phases of a certification	• Provides company-wide attestation of employee access rights and privileges required for IT best practices and compliance-related audits (SOX, HIPAA, GLBA, ISO 27001, PCI, and others)
Fuzzy ID and the Identity Mapper	• Links users from disparate applications when no consistent login ID exists • Proprietary name-matching algorithms automatically identify the same user in multiple systems with no common attribute	• Solves one of IT's largest challenges, how to view access rights when no common attributes exist • Eliminates the need to modify applications to insert a unique identifier • Establishes a single repository of all access data across the entire enterprise
Role-Based Certifications and Role Definition Tool	• Defines roles and role memberships • Performs certifications by roles and exceptions to improve accuracy and relevance • Performs what-if scenarios to define cross-application enterprise roles	• Improves relevance of certifications by reviewing a handful of roles instead of hundreds of privileges • Defines and manages roles by comparing role memberships and exceptions
Consolidated View of User Access Rights	• Custom reports show real-time and historical data • Orphaned user accounts from transfers and terminations are detected and reported • Historical record of access rights compliance	• Reveals users with inappropriate combinations of access rights • Discovers orphaned or lost user IDs • Provides documentary evidence of meeting access-related compliance controls
Real-Time Access and SOD Alerting	• System monitors for changes to user access data • Simple interface for configuring custom alerts and actions • Comprehensive cross-application separation of duties reports and alerts	• Generates alerts if access data has changed since the last audit scan • Detects unauthorized changes to systems • Warns business owners if users violate separation of duties rules
Automated Discovery	• User access rights and group memberships are automatically discovered and processed • Support provided for wide variety of commonly used applications without product customization	• Consolidates user data from diverse systems and groups by user and application • Enables Access Auditor to provide a near real-time view of user entitlements

Security Compliance Corp

Security Compliance Corporation

120 Village Square, Suite 76
Orinda, CA 94563
(866) 657-4550
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Security Compliance Corporation's (SCC) Access Auditor® automates the periodic review and certification of user access rights and entitlements. SCC's workflow engine provides the ultimate flexibility in defining and managing the periodic attestation of user access rights. The enhanced Identity Mapper™ utilizes a proprietary algorithm to link user accounts from disparate systems back to the correct person, even when common identifiers or login IDs do not exist. Access Auditor's consolidated view of user access rights enables customers to identify orphaned accounts left behind from terminated users, thus reducing the risk of fraud and audit findings. By automating labor-intensive tasks related to user access rights and separation of duties, SCC's customers improve security while minimizing the costs of compliance. Founded in February 2005, Security Compliance Corporation is based in Orinda, CA.