CASE STUDY: Children's Hospital Los Angeles - Simple Entitlement Reviews with Access Auditor®

The Challenge

CHLA needed to simplify the entitlement review process for managers, and automate the identification and removal of user accounts left behind from terminated users.

The Solution

Access Auditor automated the re-certification process and CHLA was able to launch entitlement reviews with the push of a button.

The Results

CHLA replaced a time-consuming, manual process with Access Auditor's automated imports. The Fuzzy ID and Identity Mapper enabled the hospital to create a true identity warehouse.

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

Background

Children's Hospital Los Angeles (CHLA) has been named the best children's hospital on the West Coast and among the top five in the nation for clinical excellence with its selection to the prestigious U.S. News & World Report Honor Roll. Children's Hospital is home to The Saban Research Institute, one of the largest and most productive pediatric research facilities in the United States. Children's Hospital Los Angeles is also one of America's premier teaching hospitals through its affiliation since 1932 with the Keck School of Medicine of the University of Southern California.

Children's Hospital Los Angeles needed to streamline their control and auditing of user access rights on key business applications. With thousands of users across the hospital, the entitlement review procedure was a very time-consuming and tedious manual process. CHLA deployed Access Auditor from Security Compliance Corporation (SCC) to automate the discovery, collection, and review of user access rights. Using the Identity Mapper™ and Fuzzy ID, CHLA created an identity warehouse that gave complete visibility into who has access to what. Moreover, managers and business owners can complete their user access reviews using a simple web application, rather than send email and spreadsheets to each individual and track who has completed their attestation.

The Challenge

Children's Hospital Los Angeles must protect the private health information (PHI) of countless children. In compliance with HIPAA privacy rules, the CHLA Information Security team maintains controls over access to patient data, and reviews those access rights on a regular basis. Since these audits were performed manually, the challenge facing CHLA was enormous.

Data from each application across the hospital was compiled by hand. A unique spreadsheet was produced for each employee's manager and sent to them via email for review and approval. Follow-up to the reviews was likewise manual, taking countless hours to complete. Doug Kajiwara, Information Security Manager at CHLA, sums it up: "The process was very resource intensive. Staff had to be focused on access reviews only as they were an audit requirement. We needed to have specialized expertise to be able to know that a certain job description fit a certain user profile and to be able to correlate users in various systems where there were only IDs, not user names."

With over 5000 employees, reviewing user access rights would be a monumental task even under the best of conditions. The following requirements were identified for an access rights certification solution:

- Simplify the entitlement review process for managers. The new process needed to be easy to learn and use. Large identity-management suites were therefore not a good fit and the hospital needed a simple and targeted solution.
- Improve automation and accuracy. Use fewer resources to compile the information for distribution and to make it more accurate.
- 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. Like with most organizations, various applications do not share a common login ID. At CHLA, names could be misspelled or more than one user would share the same name. The challenge of linking accounts from various systems was a critical requirement. The solution needed to be able to map all identities to each individual user.

Children's Hospital Los Angeles' requirements were similar to most companies. User entitlements were managed independently across multiple systems and without a common identifier. The access review process was highly labor-intensive and needed a simple-to-use solution.

The Solution

Doug Kajiwara wanted a solution that would streamline the entitlement review process and save his team much needed time and effort managing the reviews. Access Auditor from Security Compliance Corporation was just what the doctor ordered for CHLA.

Access Auditor provides a simple and easy-to-use solution for managing user access reviews. User data from across the company can be imported in a matter of minutes. CHLA was able to quickly import data from key health information systems. Each system has data in a different format, and CHLA is now able to create an accurate report of who has access to what. According to Doug Kajiwara, "Access Auditor was able to import various types of data in various formats. We were able to use the built-in logic to create an accurate report. We were very deliberate so that we could understand all of the data points and how we wanted to present the information to our management. Managers commented how it was much easier to use and made the process

> *"With Access Auditor, we were able to replace our manual process and succeed with periodic access reviews for management across the hospital. Access Auditor's simple and intuitive approach was a big win for CHLA."*
>
> **Doug Kajiwara, Information Security Manager**

intuitive. Our two largest goals are to be able to complete these access reviews for all managers in a periodic manner. Without Access Auditor, that would not be conceivable with our previous manual process.”

To perform user access reviews, you need to build a consolidated profile of each person across the organization. SCC’s Identity Mapper and Fuzzy ID contain a proprietary pattern-matching algorithm that allows customers to automatically link user accounts from various systems. After using the Fuzzy ID, CHLA had a centralized repository detailing who has access to what across the company, including each person’s different login.

With this new Identity Warehouse, Children’s Hospital Los Angeles was able to launch entitlement reviews with the push of a button. Customized emails were sent by Access Auditor to inform and remind approvers of their pending reviews. Reports are available for both real-time status as well as the new evidence of compliance for audits.

The Results

Children’s Hospital Los Angeles achieved excellent results. 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 Fuzzy ID and Identity Mapper enabled the hospital to create and maintain a true identity warehouse.

With the data warehouse created and automatically kept up-to-date, CHLA was able to invest in data cleanup and gain better visibility into user access rights. The CHLA staff knows who has access to what at all times and can quickly identify if user accounts were not removed for terminated staff.

The previous labor-intensive review and certification process was replaced with Access Auditor’s simple web-based entitlement reviews, resulting in a savings of countless staff hours. The hospital can now launch reviews with the click of a button and include managers and business owners without sending a single spreadsheet.

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.

Kajiwara summarizes the success for Children’s Hospital, “With Access Auditor, we were able to replace our manual process and succeed with periodic access reviews for management across the hospital. Access Auditor’s simple and intuitive approach was a big win for CHLA.”

“Access Auditor was able to import various types of data in various formats… Managers commented how it was much easier to use and made the process intuitive…that would not be conceivable with our previous manual process.”

Doug Kajiwara, Information Security Manager

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

SCC
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 2005, Security Compliance Corporation is based in Orinda, CA.