

CASE STUDY

Securing Multi-Entity Access Without Compromising Compliance

A multi-entity pharmacy organization needed a secure way for shared staff to access separate IT environments without violating compliance or disrupting critical pharmacy systems.

Operating across five independently structured pharmacy entities, the organization faced a unique IT balancing act: maintain strict separation between environments for compliance while enabling shared employees and IT staff to work efficiently across all systems. Each entity operated on its own infrastructure, yet internal teams frequently needed access to multiple networks—often from the same device. This complexity was further compounded by pharmacy software that required local network access, limiting flexibility for remote work and creating operational friction.

Without a unified access strategy, the organization risked inefficiencies, increased support demands, and potential security gaps. Shared users navigating multiple environments from a single machine introduced the possibility of crossover exposure—an unacceptable risk in a highly regulated healthcare setting.

A Secure, Unified Access Framework Built for Complexity

To resolve these challenges, a Secure Access Service Edge (SASE) approach was introduced using Cytracom Control One. Rather than consolidating environments and risking compliance violations, the solution established a secure overlay network that preserved the independence of each pharmacy entity while enabling centralized access control.

This architecture allowed users to connect securely based on identity and role, ensuring they could only

access the systems relevant to their responsibilities. Network segmentation and user-based policy enforcement became foundational components, eliminating the risk of unauthorized crossover between environments while maintaining a seamless user experience.

The deployment process uncovered an additional complexity: multiple users accessing different environments from the same shared workstation. This scenario required functionality beyond the platform's standard configuration. Through direct collaboration with the vendor's development team, enhancements were introduced to support multi-user workflows on shared devices. Additional refinements were also made to content control features, ensuring consistent performance across user sessions.

Seamless Access, Stronger Security and Measurable Impact

The result was a transformation in how the organization managed access across its distributed pharmacy network. Employees could now securely connect to the appropriate environment—whether onsite or remote—without disruption to their workflows or reliance on cumbersome workarounds.

Equally important, the organization maintained full compliance with regulatory requirements by preserving strict separation between entities. At the same time, IT operations became significantly more streamlined through centralized management and policy control.

CASE STUDY

The impact was immediately visible. Access-related support tickets declined, downtime was minimized, and shared staff experienced a more intuitive and transparent login process. The ability to continue using existing pharmacy software without modification ensured business continuity and avoided costly system changes.

Beyond operational improvements, the collaboration with the vendor delivered long-term strategic value. By helping shape enhancements to the SASE platform, the organization positioned itself as an early adopter of advanced secure access capabilities tailored to complex, multi-entity environments.

Move forward with **The Color of Confidence®**.