

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



PAT DARIENZO CISO, CATHOLIC HEALTH SERVICES OF LONG ISLAND

HEADQUARTERS: Long Island, NY

EMPLOYEES: 17,500

REVENUE: \$2.3 Billion

“The healthcare industry is at a crossroads,” says Pat Darienzo, the CISO of Catholic Health Services of Long Island (CHSLI). Darienzo continues, “There is an industry-wide priority on the sharing of patient data to make information available in order to enable the best care possible for patients. We strive to give access to those who might need it, while at the same time HIPAA requirements limit who can have access to data and place strict requirements for identity and access management.” The current landscape creates a challenging balancing act for a multitude of security leaders at hospitals and healthcare networks, especially for streamlined, distributed healthcare services organizations like CHSLI.

Darienzo emphasizes the productive approach to information security at CHSLI, solidified by the CIO and CEO, who also both recognize this important focus. “This past year was very sensitive in healthcare. In the past, information security projects declined based on budget restrictions, now it seems that sometimes the only programs that do not get cut are security programs.” This movement toward sufficient

budget along with the corresponding elevated concerns is evident at CHSLI, with Darienzo being a major advocate behind this shift.

When Darienzo took the CISO role, the security staff was small with a primary focus on tickets and access management. Darienzo coordinated a full policy rewrite soon after he arrived and helped restructure the organization to enable his team to spend their time on other priorities. This fundamental change not only resulted in a high performing team but also boosted morale and quality of results.

A core goal for Darienzo’s team is implementing a new access and identity management tool that will help the provisioning team grant and manage role-based access. He says, “CHSLI’s current process is good but it could always be better. It requires human intervention to trigger it, which can be a problem if a manager is busy or forgets to update us. If a person leaves the company the manager must send a note, otherwise the person’s access may not be removed. Our new IAM solution will integrate with

the Human Resource system so all access is revoked automatically on the employee's last day. Also, many non-employees work at CHSLI, and with this system we can run a check on their status every 90 days in order to ensure we keep access rights current."

A large portion of CHSLI's security focus is on employees and how they interact with patient data, reinforcing the importance of Darienzo's team in keeping employees informed about the value and importance of security efforts. Each employee receives security training during on-boarding and the security team publishes a monthly newsletter on their intranet. He explains to new employees, "Our security processes are the primary defense standing between CHSLI and an incident affecting our patients and business." CHSLI does not evaluate employee security awareness via specific tests, yet Darienzo consistently sees an increase in reports of suspicious emails and messages, a strong sign the organization is evolving to become more security conscious.

MEETING HIPAA REGULATIONS REQUIRES A TEAM APPROACH

CHSLI includes six hospitals, three skilled nursing facilities, a regional home nursing service, hospice and a multiservice, community-based agency for persons with special needs. Darienzo works with a team of appointed privacy and security officers at each entity. "They are our satellite arms and our first point of contact if any security incidents come up. They file incident reports with us and we conduct the analysis." Darienzo balances his time between officers, while maintaining productive ties with each.

For the purpose of reporting HIPAA incidents to the Office of Civil Rights (OCR), each incident is assessed by the CHSLI's HIPAA Executive Steering Committee, which includes Darienzo, the CIO, the CPO, the CMO and representation from the Legal Department. The group reviews all incidents and determines if a breach requires reporting, or if an additional formal risk assessment is needed. All decisions of whether or not an incident meets the definition of a breach are documented, along with the facts upon which the decision was made. In cases where the OCR has reviewed CHSLI's assessment of an incident, Darienzo states they have supported the CHSLI decisions.

BE NIMBLE AND BALANCED TO BE EFFECTIVE WITH A SMALL BUDGET

Darienzo states, "CHSLI is half the size of the Health System I had worked at prior to this position. So, while we do not have as many resources, we are more nimble. You can do a lot with less, if you focus on the right things. Some of the things we accomplish are astounding when you compare it to our annual spend."

Darienzo emphasizes the importance of a team consisting of smart and efficient people, but he is cognizant of not over-working his security team. He says, "I am here to clear hurdles for them and help them get their job done. To some extent I would say I try to be hands off with my team. I just focus on giving them the time and room to get their job done effectively." Darienzo is also trying to see that steps are taken within the security plan to give the team ample support when possible. One project that will help his team this year is a SIEM project, which will provide more comprehensive monitoring; Darienzo is essentially outsourcing that function so his team can focus on higher caliber priorities.

Pulling a Rabbit Out of the Hat

Some days CISOs may feel like security requires a 'magic touch', something with which Darienzo would agree. While his full-time career is a healthcare CISO, he is also financially supporting his magic hobby with regular performances as a magician. To Darienzo, a clear connection exists between magic and information security, a possible reason why many of the CISOs he meets also enjoy partaking in the hobby (coincidentally, the CHSLI CISO before Darienzo was also a magician). Darienzo says, "Magic is about deceiving people. You draw their attention to one spot, while you perform some sleight of hand where they're not looking. Security is the same thing, you have to be aware of what is going on beyond your line of sight. Both security and magic are about deception and it's a skill knowing how to spot that deception."