



DIVERSIFIED HEALTH CARE

AFFILIATES CASE STUDY

*By hardening their network, we ensured a clean bill of health on one firm's client-mandated security audit.*



## 1 Problem

DHCA needed access to cutting-edge security experts to keep up with rapidly evolving threats and close security gaps revealed during a security assessment.

## 2 Solution

Makaye Infosec assigned a dedicated virtual CIO and created a roadmap to closing security gaps through on-going monitoring/protection services, formal policy development, and employee education.

## 3 Benefits

- Better security: Hardened the network against cybercriminals
- Provable compliance: Able to demonstrate they have hardened their network and can maintain all mandatory network security protocols
- Satisfied audits: Passed a surprise audit initiated by one of their clients

## OVERVIEW

Diversified Health Care Affiliates Inc. (DHCA) helps keep its customers in the healthcare sector financially healthy through complete revenue cycle management programs. As part of its strict and deeply held code of conduct, DHCA considers the confidentiality and privacy of its clients and their patients to be a hallmark of their operation. To that end, they have established administrative, technical, and physical safeguards to protect clients and their proprietary information and uphold compliance requirements related to the Health Insurance Portability and Accountability Act (HIPAA).

That includes network safeguards as well, but in an era of explosive growth in cyber-attacks, DHCA was concerned its in-house network security expertise was no longer meeting the demands of modern cybersecurity. “We had people doing good work, doing the best they could,” says DHCA Executive Vice President Christian O’Connor, “but through a security assessment, we saw there were gaps.”

## CHALLENGE

In short, DHCA realized they wanted their network security as hardened as the other





elements of their best-in-class privacy and confidentiality programs, especially after an audit made clear that gaps in their network security apparatus could potentially put them at risk. The need for hardened network security was just emphasized after a customer came to them with their own surprise security audit.

DHCA was well aware of the cyber threats looming in their market. “Cyber-criminals are everywhere trying to penetrate your networks,” says O’Connor. But staying current with an ever-changing cybersecurity landscape is a major challenge, even for organizations with experience in privacy and security practices.

## **SOLUTION**

DHCA started with a security assessment from Makaye Infosec to get a clearer understanding of their security maturity and vulnerability. That assessment was eye-opening: “We saw where the gaps were,” says O’Connor, “and then Makaye Infosec came back with a strategy to close the gaps and harden our network.”

Indeed, the security audit enabled Makaye Infosec to develop a step-by-step roadmap for DHCA to implement all mandated and recommended network security protocols.

In addition to ongoing managed security services, Makaye Infosec also helped DHCA create a bespoke set of security policies to govern company practices and guide employee behavior. Given that employees are often themselves the first and last line of defense

against cybercriminals, Makaye Infosec also provided extensive direct employee training to help them recognize and know how to react to malicious activity

Makaye Infosec’s work also required them to work closely with sister company GXA, which provided DHCA’s Managed IT Services. To have both excellent IT operations and cybersecurity requires both the IT and cybersecurity groups to work collaboratively but ideally separately. By splitting the two functions into separate responsibilities, DHCA ensures it gets the best of both worlds: “Makaye Infosec holds the IT department or MSP accountable for their roles in the comprehensive network security goals.”



As a result, when a customer came in with a surprise security audit, DHCA was able to satisfy their concerns. “Through the help of your team, we were able to demonstrate that we had all the security parameters in place to pass their requirements,” says O’Connor.

DHCA prides itself on taking the utmost care of its clients’ private information, and with Makaye Infosec’s help, they can ensure they’re hardened against the ever-changing cyberthreat landscape.



# RESULTS



## Reliable Partnership

"You actually deliver on your promises. You've also been available when needed."



## Better Risk Management

"We've mitigated multiple risks because of your proactive approach to ensure we're protected."



## Peace of Mind

"It gives me confidence to know I have a knowledgeable CIO from Makaye Infosec."



## More Aware Staff

"We have a more informed workforce because of the ongoing cybersecurity education."

"It just gives us a comfort level knowing we've got a good partner who's interested in a long-term partnership."

Christian O'Connor,  
Executive Vice President of  
Diversified Health Care  
Affiliates Inc





# Your Trusted

# Cybersecurity Partner

If you need help addressing your cybersecurity concerns, Makaye Infosec has extensive knowledge and expertise in securing and protecting healthcare partners.

Contact us today for a **free consultation** and find out how a **Cybersecurity Maturity Assessment** can help you secure your organization and achieve HIPAA compliance.



**George Makaye, CISSP**  
**[smla@minfosec.com](mailto:smla@minfosec.com)**  
**(972) 645-2218**  
**[www.minfosec.com](http://www.minfosec.com)**