INTRODUCTION

As Aurora Mental Health Center prepares to build on its new Acute Care Campus, Cripps sat down to reflect on how the organization has approached cybersecurity during a period of profound change.

Now in its 50th year, Aurora is navigating a transformation shaped by growth, community need, and a digital threat landscape that touches every part of care delivery.

> *“Last year we celebrated our 50th anniversary,” Cripps said. “Our doors opened in 1975. When we originally opened, it was a much smaller clinic. Now we're able to have 700 staff.”*

Aurora's growth mirrors the complexity of the community it serves. Located in one of the most diverse zip codes in the country, the organization delivers behavioral health services across schools, homes, jails, and community settings, serving clients in more than 40 languages. That diversity, Cripps noted, shapes everything from care delivery to operational risk.

> *“We serve everyone from kiddos to older adults, we are based in community systems such as schools and jails, and in January we opened our new Acute Care Campus with our crisis and detox services,” she said.*

With that breadth comes responsibility and exposure. **Behavioral health organizations** have become a focal point for cyber adversaries targeting specialty care providers, drawn by highly sensitive data, decentralized systems, and vendor-dependent environments that create multiple paths for exploitation.

Therapy notes, psychiatric records, and data related to children carry not only regulatory weight, but deep personal and social consequences when exposed. Recent incidents across behavioral health and specialty care illustrate the stakes: ransomware

campaigns initiated through compromised remote access, large-scale data exposure tied to third-party weaknesses, and repeated extortion attempts that disrupt operations and delay care.

> *"It used to be financial information," Cripps said. "But now people want behavioral health data, especially data related to children."*

CONTEXT

The Rising Risk Facing Behavioral Health

For years, funding uncertainty, workforce shortages, and administrative burden have been familiar challenges in behavioral health. What has changed, Cripps believes, is speed.

> *"The pace of change now is so much faster than it was five years ago, and it's astronomically faster than it was ten years ago."*

Cyber threats evolve faster than internal teams can reasonably keep up with, particularly for organizations that must balance fiscal responsibility with patient care. Against that backdrop, Aurora faced a fundamental question: how to strengthen security without making already difficult jobs harder.

LEADERSHIP PHILOSOPHY

Technology as a Tool, Not the Center

Cripps, who recently stepped into the role of Chief Information and Innovation Officer, says IT leaders have to approach technology differently than they did 10 years ago. “Technology is intertwined with most operations now and we have to understand how it all flows together,” she said.

> *“I love that our job in IT is to try to improve things so our staff and clients have a better experience. IT is a process improvement division and technology is a tool we can use when appropriate.”*

That philosophy shapes how Aurora evaluates security controls. For Cripps, success means finding the balance between protection and practicality. She is wary of security measures that look good in theory but fail in practice for users.

> *“If security makes people's jobs harder, they'll find a workaround. The nuance is how it actually fits the work we're doing.”*

One example came in the form of email encryption, a requirement in healthcare, but historically a source of frustration. “For a long time, you had to remember to type ‘secure’ in the subject line or click a button,” Cripps explained. “That's not realistic in healthcare.”

The consequences were tangible.

> *“We had multiple providers threaten to quit if we didn't figure out the old way that we were doing encrypted email because it was inhibiting care. That's not helpful.”*

The solution wasn't less security, but better-designed security, with protection that worked automatically in the background, safeguarding sensitive information without disrupting care or communication. Security controls that added friction risked being bypassed; security that was thoughtfully designed could protect privacy while allowing clinicians to stay focused on patients. “That was an enormous win,” Cripps said.

TURNING POINT

A Tipping Point to a New Partnership

Aurora's cybersecurity journey reached an inflection point when long-time institutional knowledge began to retire. At the time, Aurora was still largely self-hosting its infrastructure, which was a heavy lift for a small IT team.

Rather than simply replacing what they had, Aurora paused and asked a bigger question: was this the right moment to rethink everything?

> *"Is now a good time to completely pivot? Not only did we decide we should not build a fancy data center in this building, we should start moving to the cloud."*

Aurora spent nearly a year evaluating options, speaking with organizations large and small. For Cripps, the process was as much about education as selection. What ultimately mattered was comprehensiveness.

AURORA'S PATH TO A CLOUD-FIRST SECURITY MODEL

Self-hosted infrastructure

Aurora runs its own servers and IT environment, a heavy lift for a small internal team.

Institutional knowledge retires

Long-time staff begin to retire, forcing a decision: replace what existed, or rethink it.

Nearly a year evaluating options

Aurora speaks with organizations large and small, weighing what comprehensive support actually looks like.

ClearAdvantage partnership begins

Virtual CISO leadership, a 24/7 security operations center, and ongoing risk analysis, in one place.

Governance committee established

Cybersecurity moves out of IT alone and into Aurora's quality council, with clinical and operational leaders at the table.

Aurora ultimately partnered with **Clearwater Security & Compliance** through its ClearAdvantage program, gaining access to virtual CISO leadership, a 24/7 security operations center, and ongoing risk analysis. The goal wasn't to outsource responsibility, but to ensure the right expertise was consistently available.

> *“There is no possible way internally that we could keep up with the pace of change that's happening out there in the environment. And still be fiscally responsible.”*

RESULTS

From IT Responsibility to Organizational Accountability

Before the engagement, cybersecurity was IT's thing. With a governance committee embedded in Aurora's quality council, it became everyone's responsibility.

24/7
Security operations center coverage

3x
Budgeted for security spend that wasn't needed

1
Governance committee spanning clinical, operational, and admin teams

- → Cybersecurity moved from an IT-only decision to a standing governance committee
- → Leadership and the board gained structured, ongoing visibility into cyber risk
- → Three separate years, budgeted security spend wasn't needed after all
- → Encrypted email now works automatically, without workarounds that slowed care

"It made it a lot easier when I had to say, 'we need to spend some money here.' We could show exactly why."

With support from Clearwater, Aurora worked to formalize governance structures that moved cybersecurity out of the IT silo and into existing leadership forums, bringing together representatives from across clinical, operational, and administrative teams.

> ***"This is not an announcement meeting. It's a working group. We are responsible for this now."***

For the first time, leadership and the board had structured visibility into cyber risk: what was working, where gaps existed, and how remediation would happen. "We now have solid data," Cripps said. "We didn't necessarily have that before."

BEFORE & AFTER THE GOVERNANCE SHIFT

BEFORE	AFTER
• Cybersecurity treated as “IT's thing”	• Cybersecurity is an organizational responsibility
• Self-hosted infrastructure managed by a small team	• Cloud infrastructure backed by a virtual CISO and 24/7 monitoring
• Encrypted email required manual steps that slowed care	• Encrypted email works automatically, in the background
• Leadership lacked consistent visibility into risk	• Board and leadership see risk data and can act on it directly

Unexpectedly, the shift also saved money. “Three times now I've budgeted a decent sum of money, and we haven't had to spend it,” Cripps said. “The partnership has already paid off in ways I did not expect.”

“If security makes people's jobs harder, they'll find a workaround. Anybody can take a tool and say, ‘Here you go.’ The nuance is how it actually fits the work we're doing.”

WHAT'S NEXT

Preparing for What Comes Next

As Aurora looks ahead, efficiency and protection go hand in hand. Like many behavioral health organizations, Aurora must plan for funding volatility while maintaining care standards. “We're looking for any and all tools that help make things more efficient,” Cripps said.

Managing data makes governance, vendor management, and regulatory awareness essential, especially as new expectations emerge around AI, third-party risk, and sensitive data handling.

> *“We're not just responsible for us. We're responsible for our vendors too.”*

ADVICE FOR PEERS

You Don't Have to Do It Yourself

When asked what she would tell other leaders navigating similar challenges, Cripps was direct.

> *“You don't have to do it yourself and really, you should not at this point. Having a partner that acts as an extension of your internal teams is critical. We can't wait in line because we are a small fish in a big pond. I've been able to reach Clearwater the same day every time I've needed to, and that is invaluable.”*

She also noted how much has changed in just a few years. “Five years ago, I wouldn't have thought organizations our size could access this level of expertise,” she said. “That's changed.”

For Aurora, the goal isn't perfection. It's sustainability and security that supports care rather than standing in its way.

> *“We're trying to protect our information, while still allowing people to do the work they came here to do.”*

Clearwater partners with behavioral health and community care organizations to bring virtual CISO leadership, 24/7 monitoring, and board-ready risk data to lean IT teams, without adding headcount.

Connect with Clearwater