Why did you feel that performing a vulnerability assessment was important to your organizational infrastructure?
We work hard to keep our hardware and software up to date. An outside evaluation helped us see network security areas we may have missed. It also recommended ways we could close identified gaps.

Were you or your IT staff concerned about what this vulnerability testing might find?
We weren’t concerned—just curious and ready to respond if specific opportunities for improvement were identified. We absolutely trusted the OCHIN team to identify these opportunities in an efficient and effective way.

What was your biggest takeaway from the vulnerability assessment? Have you made any adjustments since the testing took place?
Yes. Following the vulnerability assessment, we made relatively minor adjustments. Once we received reassurance that our systems were as secure as we could make them, it enhanced our peace of mind tremendously.

Has your board or HRSA ever asked how you manage cybersecurity?
Our board members ask about our cybersecurity efforts because they see reports of ransomware and other attacks in the news. I always welcome the chance to discuss proactive measures we’re taking on behalf of our patients, our organization, and the communities we serve—so it’s well-received when I share that those measures include participating in external cybersecurity audits.

In your opinion, what’s the biggest misconception that exists in health care today regarding cybersecurity?
There’s no such thing as a small target. Even a frontier clinic like ours is potentially vulnerable. OCHIN takes extremely proactive and comprehensive measures to keep its robust technology infrastructure secure for its members. Yet even with those measures in place, engaging external assessment expertise provides objective insights that greatly enhance our organizational confidence and peace of mind. Regardless of size, organizations should also implement two-factor authentication and strong encryption protocols.

What specific advice would you offer other OCHIN member leaders about infrastructure security?
Keep it as simple to manage as possible—but also make it as comprehensive as necessary to support your scope. You don’t need the most expensive tools available. You need the most reliable tools your team can manage effectively.

To learn more about OCHIN cybersecurity assessment services, visit ochin.org/cybersecurity-assessment-services