1484 Highland Avenue / Suite 2
Cheshire, Connecticut / 06410
www.chcact.org

Testimony of

Deb Polun
Chief Strategy Officer
Community Health Center Association of Connecticut (CHC/ACT)

Commenting on
Senate Bill 403: An Act Concerning Cybersecurity

Public Safety & Security Committee
March 10, 2026

Thank you for the opportunity to provide comments on this important bill.

On behalf of the Community Health Center Association of Connecticut (CHC/ACT), and its sixteen member community health centers, I want to thank the Committee for its dedication to addressing issues around the growing concern of cybersecurity. Connecticut's community health centers serve more than 452,000 people each year, providing medical, behavioral health, dental, and some specialty care in hundreds of locations across the state.

In addition to providing education, convening, public policy and advocacy for Connecticut's health centers, CHC/ACT also hosts a Health Center Controlled Network (HCCN). Our HCCN is a federally funded program that supports twenty Connecticut and Rhode Island health centers in leveraging health information technology (IT) and data to improve clinical quality, patient-centered care, and provider and staff well-being. For our current program cycle, CHC/ACT's HCCN is focused on strengthening health centers' cybersecurity positioning to reduce the threat of attacks and protect patient data.

Comments on the proposal

1) Architecture changes: CHC/ACT supports the idea of this bill, but, like other health care providers, we have concerns about mandating architecture changes that our health centers' systems cannot easily support. Health centers operate on extremely thin financial margins, and many may not be able to afford to meet this new mandate, especially within the timeline specified in the bill. If the Cybersecurity Seed Fund is established, pursuant to section 7 of the bill, we request that grants are set aside for primary care providers to advance planning and adoption of new requirements and best practices.

2) Task force: CHC/ACT supports the creation of a State Cybersecurity Intelligence Task Force and recommends the addition of leadership from the Department of Public Health and/or health care providers, as cybersecurity incidents impact health care more than any other field. Health care systems have adopted stringent cybersecurity protections, and the actual number of breaches has declined slightly year over year. Yet the impact of the breaches has grown: in

2024, the number of affected individuals soared by 58% to more than 289 million individuals, almost 85% of the population of the United States.

3) HIPAA 2.0: Notably, health centers are already meeting federal standards around cybersecurity – standards which are poised to change with an updated Health Insurance Portability and Accountability Act (HIPAA) Security Rule (colloquially known as "HIPAA 2.0"), which is expected soon. Any legislation forwarded by the Committee should align with existing and expected standards.

We appreciate the Committee's attention to cybersecurity, as well as your consideration of our comments – and, most importantly, your hard work on behalf of our great state. Please feel free to reach out with any questions: dpolun@chcact.org or 860.667.7820.