Health Sector Coordinating Council
Cybersecurity Working Group

Health Sector Publishes Report on the Cybersecurity Plight and Needs of America's Resource-Constrained Healthcare Providers

Washington, DC – May 7, 2025 – America's resource-constrained healthcare providers face significant challenges in managing cybersecurity due to limited workforce and expertise, outdated systems, and insufficient funding, according to a report issued today by the Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group. The report – sent to the U.S. Department of Health and Human Services, the White House, and the House and Senate Rural Health Caucuses - calls on government and the broader healthcare community to support workforce augmentation, financial resources and partnerships to enhance cybersecurity and protect patient safety.

The report - "***On the Edge: Cybersecurity Health of America's Resource-Constrained Health Providers***," examines how resource-constrained health care systems - small, rural, critical access, family clinics, skilled nursing facilities, FQHCs and many more across the country - are only marginally prepared for ongoing cyber threats to clinical care and operational liquidity, and recommends forms of support they would need against stiffer cybersecurity regulatory requirements.

The healthcare industry is now targeted by more cyber adversaries seeking monetary gain than any other industry sector in the United States, and our nation's resource-constrained providers skate on the razor's edge between maintaining clinical care or going out of business from a cyber attack.

"This report accurately captures the challenges our rural hospitals face," said Tianna Fallgatter of The Rural Collaborative, which represents 28 rural hospitals in Washington State. "Already stretched too thin, experiencing increasingly sophisticated cyber-attacks, our hospitals will not be successful at protecting the nation's people without government support. We need to find a way to provide the funding urgently needed despite our nation's budget shortfalls to make rural hospitals and their patients a priority," she urged.

"On the Edge" summarizes HSCC interviews with 40 executives of small, rural, critical access, FQHC, skilled nursing facilities and more in 30 states across the country, exploring how they approach their cybersecurity responsibilities and what kind of government and community support would be meaningful to strengthening their cyber health.

Jim Roeder of Minnesota-based Lakewood Health and a co-lead of the HSCC task group that prepared the report, observed that "This report sheds a critical light on the cybersecurity challenges threatening resource constrained healthcare providers like ours. It accurately reflects the fears we face daily in knowing that a single ransomware attack could not only jeopardize our hospital's future but also put our patients and community at risk." Roeder added that "Cybersecurity is not just an IT issue; it is a patient safety issue. Protecting the health and well-being of our communities means ensuring we have the resources and support to defend against evolving cyber threats."

The *Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG)* is a government-recognized critical-infrastructure industry advisory council of more than 460 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities and government agencies partnering to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes free healthcare *cybersecurity leading practices* and policy recommendations, and produces outreach and communications programs emphasizing the imperative that ***cyber safety is patient safety.***

##

More information: *greg.garcia@HealthSectorCouncil.org*
https://HealthSectorCouncil.org/Contact