Written Testimony of Linda Stevenson

CIO of Fisher-Titus Medical Center and CHIME Board Member

Senate Committee on Health, Education, Labor, and Pensions (HELP)

“Securing the Future of Health Care: Enhancing Cybersecurity and Protecting Americans’ Privacy”

July 9, 2025

Chairman Cassidy, Ranking Member Sanders, and members of the Committee,

My name is Linda Stevenson, and I am the Chief Information Officer (CIO) of Fisher-Titus Medical Center with over 35 years of experience in health information technology (IT). I also currently serve as a Board Member for the College of Healthcare Information Management Executives (CHIME). As a CIO of a rural hospital, I hope to provide a unique perspective on the difficulty of protecting our patients in an era of constantly evolving and escalating cyber threats.

Background

Fisher-Titus Medical Center is a rural, independent hospital in Ohio that serves the greater Huron County area and its 70,000 residents with a full continuum of health and wellness services including: a 99- bed acute care hospital; a 69-bed skilled nursing facility; a 48-unit assisted living facility; a Home Health Center; and outpatient services, including laboratory, imaging, and physical rehabilitation. While the medical center itself is in the City of Norwalk, Fisher-Titus and its physician group have medical offices throughout Erie and Huron counties. Fisher-Titus is the largest provider of medical services in Huron County, as well as the largest employer.

The College of Healthcare Information Management Executives (CHIME) is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers (CIOs), chief digital officers (CDOs) and other senior healthcare IT leaders. CHIME members are among the nation’s foremost health IT experts, including on the topics of cybersecurity and privacy.

Today I will focus my remarks on the daily challenges my facility and other rural hospitals face as we experience growing cybersecurity attacks against us and our patients. These include significant resource constraints, massive workforce shortages, and unprecedented and ever-changing regulatory requirements. Taken together, it has become very hard for facilities like mine to make the critical cyber investments needed to keep pace with these attacks. Thankfully, I do believe there are ways to address these challenges which include approaches like deregulation and reducing administrative burdens, a stronger focus on policies that incent strong cyber practices instead of punishing providers who are attacked, and ongoing support for widely used cybersecurity tools. Key takeaways are summarized below with further detail throughout my testimony.

Key Recommendations and Takeaways

- Rural hospitals are significantly resource constrained. Attracting and securing cyber talent is especially difficult for small, rural hospitals. Our cyber teams are very small, and in some cases, are staffed by individuals who wear many hats.
- The healthcare sector is the most heavily regulated sector in the U.S. The operational burden of complying with overlapping and burdensome mandates can be overwhelming, especially for rural healthcare providers.
- We must shift away from punitive approaches that penalize providers who are targeted by malicious actors to policies that empower healthcare providers to strengthen their cyber defenses.
- Ongoing support for federal tools is needed. Rural hospitals cannot do this alone.
- There are significant vulnerabilities associated with third-party partners that must be addressed to protect Americans' health data. It would be helpful if providers had an approved list of vendor products that have already been vetted to help us select from which meet a baseline set of privacy and security standards.
- The legal and operational responsibility for ensuring HIPAA privacy and security compliance falls too heavily on provider organizations.

Resource Constraints

Hospitals undertake and devote significant resources to securing our systems because we are truly committed to the health, well-being, and safety of patients in the communities we serve. However, cybersecurity is costly and small, rural, and under resourced hospitals are constrained when it comes to IT by both funding and workforce shortages. Recruiting and retaining qualified IT and cybersecurity professionals remains a persistent challenge. The shift to remote work has only been exacerbated in rural areas where we are competing for talent with other, better resourced organizations across the country who lure strong candidates and talent away with higher compensation. Most rural hospitals cannot afford a full-time chief information security officer (CISO) or cybersecurity leader. At my own hospital I am both the CIO and the CISO.

Rural hospitals serve older, lower-income populations—leading to a higher reliance on Medicare and Medicaid. At Fisher-Titus Medical Center in 2024:

- Nearly 80% of inpatient admissions were patients with either Medicare or Medicaid insurance.

- A 10% decrease in commercially insured patients receiving care across the system, with an 18% decrease in these patients being admitted to the hospital.
- An 18% increase in Medicare patients being seen in the outpatient setting due to the aging population in the rural communities.
- The year closed out with a -1.1% operating loss with the facility writing off $8.2 million in charges through denials, which includes medical necessity and prior authorizations.

When hospitals face budget constraints due to stagnant payment rates, they are often forced to reprioritize spending, redirecting limited resources toward immediate operational and patient care needs and away from long-term investments like cybersecurity. This challenge is even more acute for rural hospitals, the majority of which are operating at a loss – 50% are in the red in 2024, up from 43% the previous year.[1] Their ability to make strategic investments in cybersecurity and workforce is severely limited. While mid-to-large hospitals typically allocate 6-10% of their IT budgets to cybersecurity, small and rural hospitals spend closer to 4%, further underscoring the disparity in their ability to defend against cyber threats.[2]

Compounding these challenges is a rapidly evolving cyber threat landscape, where criminals are weaponizing AI to launch increasingly sophisticated attacks. Without the funds and access to a vibrant cybersecurity workforce, rural hospitals will continue to struggle. A catastrophic cyber-attack can bring a hospital down for weeks or even months. If we were forced to divert patients, the three nearest hospitals are each roughly an hour away. In rural communities like ours, this can have devastating and potentially life-threatening impacts on patient care.

Regulatory Burden

The healthcare sector is the most heavily regulated sector in the U.S. with administrative costs accounting for 25–33% of total healthcare spending.[3] The operational burden of compliance with multiple overlapping and burdensome mandates can which be debilitating for a rural healthcare provider. Rural hospitals must meet the same standards as larger facilities but often lack the staff and infrastructure to do so efficiently. Examples of these policies include Health Insurance Portability and Accountability Act (HIPAA), information blocking mandates under the 21st Century Cures Act, Medicare Conditions of Participation, Section 1557 of the Affordable Care Act focused on ensuring equal access to care, and the Medicare-mandated SAFER guides.

[1] chartis_rural_study_pressure_pushes_rural_safety_net_crisis_into_uncharted_territory_feb_15_2024_fnl.pdf
[2] Hospitals at Cybersecurity Crossroads: Projected Medicaid Cuts Threaten 25% of U.S. Hospitals - Black Book Research
[3] Reducing administrative costs in US health care - The Hamilton Project

Providers also experience significant burdens navigating Medicare Advantage plan policies including higher rates of denials, payment delays, and prior authorization requirements, all of which put undue hardship on hospital staff, further driving up healthcare costs. For Fisher-Titus Medical Center, Medicare Advantage Plans make up 53% of our total Medicare payer mix, compared to 47% with traditional Medicare insurance. These plans reimburse nearly 10% less than traditional Medicare, equating to $5.7 million less reimbursement in 2024.

Providers are also deeply concerned about the HIPAA security proposed rule issued by the Biden administration in December. If finalized, this rule could cripple healthcare providers across the board and drive more rural providers out of business. It would be helpful for lawmakers to weigh in with the U.S. Department of Health and Human Services (HHS) about the exceptionally burdensome nature of this rule and advocate for it to be rescinded. CHIME's detailed comments on this rule can be found here.

Rural hospitals are struggling under the crushing weight of these existing policies and thus support efforts to reduce and streamline regulatory burdens. There are policy changes that could reduce the burden on rural hospitals and bring more efficiency to the overall system. Many providers are already required and eager to share patient data to improve patient care across the continuum. However, this process is difficult and burdensome with the lack of standardization across the industry. An example of this would be a customized and costly interface between our organization and a payer. Requiring all healthcare entities (providers and payers) to follow the same standards would improve population health and continuity of patient care.

Federal Tools

Rural hospitals, like Fisher-Titus, continue to make investments to improve our cyber posture, but we cannot do it alone. Ongoing support for federal tools is needed. We follow the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), as well as the 405(d) tools (i.e. Health Industry Cybersecurity Practices (HICP)) which are linked to the NIST CSF. We also regularly use materials developed by the Cybersecurity & Infrastructure Security Agency (CISA).

405(d), a voluntary set of cybersecurity best practices required under the Cybersecurity Information Sharing Act of 2015 (CISA 2015), were co-developed between healthcare stakeholders and federal authorities under the Health Sector Coordinating Council's (HSCC) Cybersecurity Working Group and published by HHS. These tools have been immensely helpful to my organization and many other rural healthcare providers. The work that went into developing them is a shining example of a strong public-private partnership. Unfortunately, there is uncertainty surrounding the future of these voluntary standards with the reorganization of HHS. Anything lawmakers can do to ensure HHS continues to prioritize this program would benefit rural providers.

Fisher-Titus is also a member of the Health Information Sharing and Analysis Center (H-ISAC), which shares timely and actionable cybersecurity threat intelligence. This is an incredibly helpful tool in our cybersecurity toolbox, however, the cost of membership may be out of reach for some rural facilities.

Rural hospitals would benefit from dedicated and ongoing funding to implement cybersecurity best practices. That's why it was encouraging to see the introduction of the Health Care Cybersecurity and Resiliency Act of 2024[4] by the Senate Health Care Cybersecurity Working Group last Congress. This bill takes an important step forward by allowing HHS to award grants to eligible entities for the adoption and use of cybersecurity best practices. At the same time, it's important to recognize some of the challenges rural hospitals face in accessing these opportunities. Grants can be costly for rural facilities to pursue, since many of us (Fisher-Titus included) do not have dedicated grant writing staff. Additionally, the time-limited nature of grants make it difficult to support long-term cybersecurity investments. These are considerations that I hope HHS keeps in mind when implementing such a program.

Last year, HSCC convened a workgroup to hear directly from resource-constrained providers across the country about their cybersecurity challenges and needs. One key recommendation that I support to ease the burden of navigating funding opportunities is to have HHS create a comprehensive list of federal subsidies and grants across the government that fund cybersecurity services, tools, and education.[5]

Incent-driven policies

Healthcare providers are too often punished rather than being treated as a victim when cyberattacks occur. Every day, we are on the front lines, fending off increasingly complex and relentless intrusion attempts. The reality is, we are up against well-funded criminal groups and even nation states that have far greater resources than most U.S. hospitals and health systems. It's no longer a matter of *if* an attack will happen, but *when*.

We must shift away from punitive approaches that penalize providers who are targeted by malicious actors. These only worsen the burden and divert resources away from patient care. Instead, we need supportive policies that empower healthcare providers to strengthen their cyber defenses. Public Law 116-321[6], passed by Congress and signed into law by President Trump on January 5, 2021, is a perfect example of a law that rewards rather than punishes healthcare providers who are taking proactive steps to

[4] https://www.help.senate.gov/cyber-wg-bill-textpdf
[5] On-the-Edge-RESOURCE-CONSTRAINED-HEALTHCARE-CYBERSECURITY.pdf
[6] PUBL321.PS

strengthen their cyber posture. Among the tools that providers can get credit for using are the 405(d) cybersecurity best practices. Continued support for this law is critical, but oversight is needed to ensure its implementation aligns with Congressional intent. Furthermore, the HIPAA Security Proposed Rule appears to run counter to the intent of this law.

The Centers for Medicare and Medicaid Services (CMS) and the Office of the Inspector General (OIG) took an important step by instituting cybersecurity donation policies under the Stark and Anti-kickback rules during President Trump's first administration in December 2020. Sadly, these policies have been underutilized by rural hospitals due to lack of clarity, awareness, and misunderstanding of applicability. With some simple changes, these policies could significantly improve rural providers' cyber posture. Congress should work with CMS, OIG, and other stakeholders, like CHIME, to explore how to best update them.

Third-Party Risk

Providers are also wresting with significant vulnerabilities brought on via third-party partners that must be rectified to secure Americans' health data. Having to ensure the security programs of hundreds of external partners is resource intensive for all, but especially for rural hospitals. Providers need assurance that the technology they are purchasing is secure, however, without a single set of standards that must be met, providers are left having to run their own security risk assessment when purchasing technology like medical devices, applications, and AI. We simply do not have the resources to undertake our own risk assessment for each product we purchase.

Given how resource-constrained we and other rural hospitals are, it would be incredibly helpful if we had an approved list of vendor products that have already been vetted to help us select from which meet a baseline set of privacy and security standards. This would bring efficiency to the marketplace and help under-resourced providers like small and rural entities purchase third-party services with greater confidence.

Privacy Challenges

As a preliminary matter, it is impossible to have privacy without security and every security breach is a privacy risk. From my perspective, anyone handling health data should be required to protect it. Given the complexity of managing health data as well as the number of entities that have access to health data, this area is clearly in need of reform. There are two areas in particular that I want to highlight.

First, when it comes to the legal and operational responsibility for ensuring HIPAA privacy and security compliance, the burden falls too heavily on provider organizations. Even though business associates (BAs) are bound by contract to protect patient data, some entities are not meeting their legal obligations which strains rural facilities.

Typically, larger BAs use a take it or leave it approach. They are unwilling to make changes to business associate agreements (BAAs) and due to our size we have a much harder time negotiating contracts. It is our experience that many business associates simply do not have robust HIPAA privacy and security programs to protect the privacy of our patients. Therefore, the burden for ensuring that our BAs have appropriate protections in place rests on our shoulders. We do not have the resources to manage this, and if we are unable to prove we are auditing our BAs, we can be fined by HHS.

Second, given the regulatory and legal landscape associated with managing health data, I strongly support the need for a national and comprehensive privacy law that protects consumers' sensitive health information without duplicating existing HIPAA requirements. Rural healthcare providers face challenges due to the complexity associated with meeting state and federal privacy laws which include treatment of children’s health data, pharmaceutical requirements, and sensitive health data like behavioral health and substance abuse. Managing the complexities associated with protecting patient’s health data is resource-intensive for Fisher-Titus and other rural hospitals. This has grown increasingly complicated when you layer on the information blocking policies that often run contrary to HIPAA. A national privacy law should require anyone with access to health data to share the responsibility for securing and protecting it.

Conclusion

In closing, I would like to thank the Committee for giving me the opportunity to testify on this important issue. With more knowledge and understanding of the realities of healthcare in our rural communities, we can work together to improve care for all. I look forward to answering your questions.