Executive summary

This report examines where rural healthcare is falling behind on cybersecurity and what that means for the rest of the industry.

The data is clear: rural teams need tools that work out of the box in small, resource-limited environments. They need security tools that work for them by default, because right now too many tools are working against them, and attackers are taking notice.

Rural healthcare providers deliver care to millions of Americans, but when it comes to email security, they often operate with one hand tied behind their backs. New research from Paubox reveals that these organizations face steeper infrastructure challenges, tighter staffing constraints, and greater barriers to adopting the tools they need to protect patient data than urban providers.

These challenges widen the vulnerability gap that leaves critical care systems and protected health information (PHI) exposed. While cybersecurity attacks increase across the entire healthcare sector, rural providers shoulder a disproportionate share of the risk, and they have far less support to address it.

KEY INSIGHTS

9 out of 10

say secure email is critical to maintaining patient trust, yet 85% report that their current infrastructure can't support advanced email security.

50%

of rural respondents cite budget limitations as a top barrier to adopting HIPAA-compliant email, nearly double their urban peers.

22%

Rural orgs are lagging their urban counterparts by 22% in adopting AI-driven threat detection

73%

of rural leaders admit they struggle to maintain HIPAA compliance due to a lack of staff and funding.

PAUBOX EMAIL SUITE

Talk to us about secure email that doesn’t depend on wishful thinking

- Setup in 15 minutes
- HITRUST certified since 2019
- No portals, no passwords
- Top rated U.S. support

Let’s chat!

PAUBOX