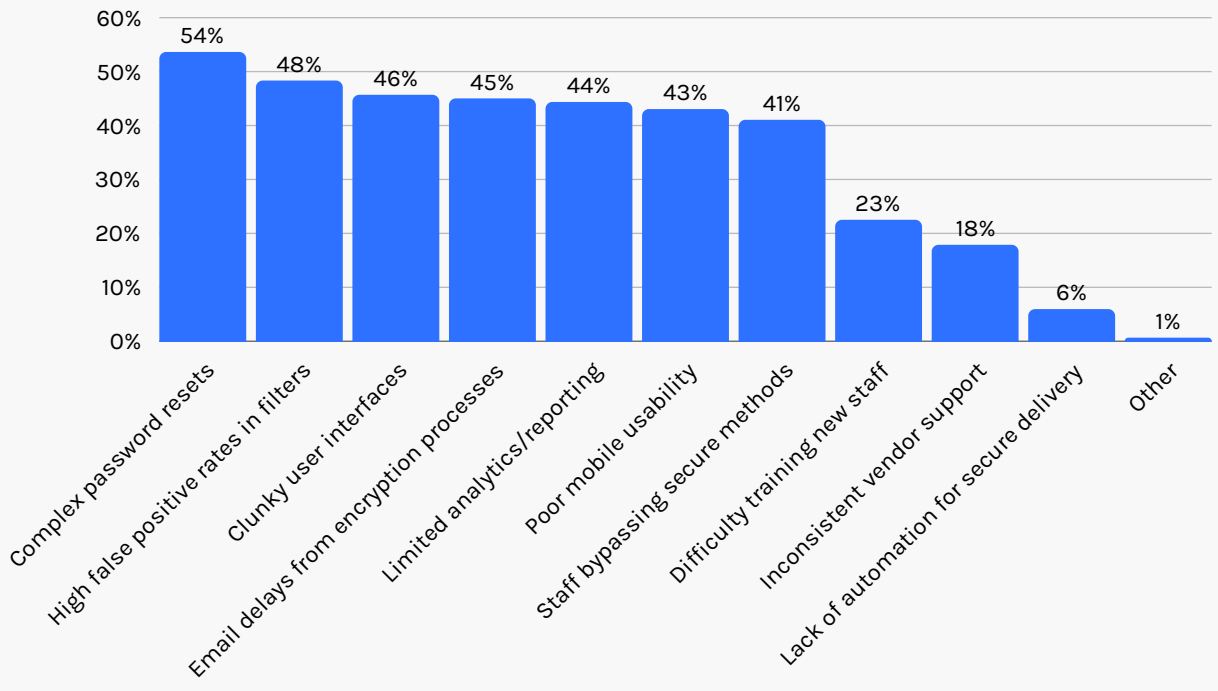
When security plans create friction

If an email security system creates frustration, it will be bypassed. We've seen it time and again—patients giving up on portals and administrators manually sending PHI because the official system is too slow.

86% of IT leaders say their current tools cause workflow friction.

These tools were supposed to help—but too often, they get in the way. The best ones? You don't even notice they're there. Tools that make secure communication seamless—not stressful—are the ones that actually work.

TOP FRUSTRATIONS WITH EMAIL SECURITY TOOLS



Complex logins. Forgotten passwords. Delayed access. These aren't minor usability bugs. They're reasons users go rogue.

We've heard it all:

- "Patients keep calling saying they can't open the message."
- "Our funders asked us to resend reports another way."
- "Our doctors are just texting files instead."

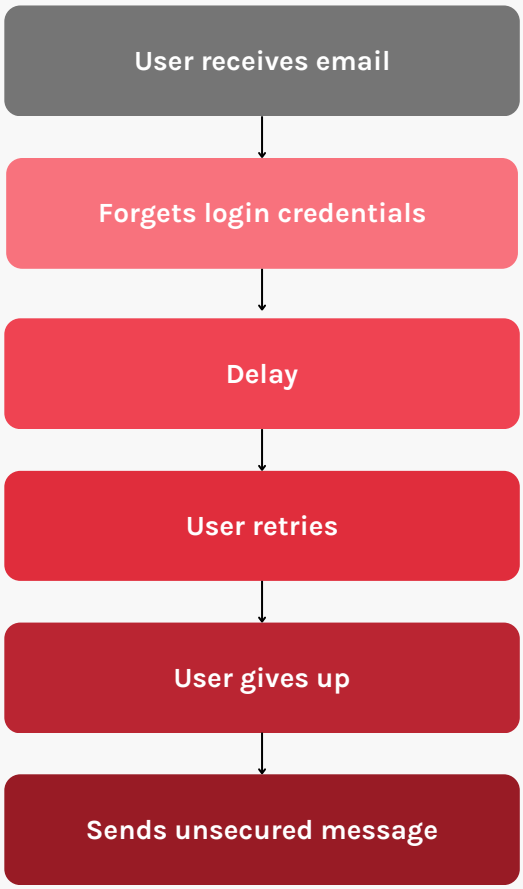
This is the inflection point: do we keep tolerating broken systems in the name of tradition? Or do we admit that usability is part of security—and build for both?

One tool designed with both usability and protection in mind is Paubox's ExecProtect+. By blocking display name spoofing and phishing attacks before they reach employee inboxes, ExecProtect+ removes the burden from end users entirely. It works in the background—no portals, no extra steps—giving healthcare organizations the security they need without adding friction to everyday workflows.

KEY TAKEAWAY

The most secure email system is the one your users actually use.

WHAT HAPPENS WHEN SYSTEMS GET IN THE WAY



> "Our company is as strong as the weakest employee link. HIPAA compliance depends on awareness and proper training—but also the right systems."
>
> **Ryan Winchester**
> Director of IT, CareM

Misconceptions are constantly undermining effective email security. Too often, healthcare IT leaders rely on outdated beliefs—assuming that compliance equals protection, that staff training alone can stop phishing, or that buying a HIPAA compliant tool checks all the boxes. But assumptions don't stop breaches. In reality, what sounds secure on paper often falls apart in practice—especially when systems create friction, rely on human behavior, or aren't fully configured. The myths are persistent, but the stakes are too high to let them go unchallenged. Below, we break down the most common false beliefs, and the facts that every security leader should know.

MYTH	FACT
"Portals equal compliance."	Most portals introduce friction—leading to non-compliance workarounds.
"Our staff are well-trained, so we're secure."	Human error is inevitable. You need tools that compensate, not just train.
"Email is just a communication tool."	Email is your most common PHI exposure point—and your biggest risk.
"More training will solve our readiness against phishing attacks."	Training helps, but 95% of phishing still goes unreported. You need better detection.
"Buying a HIPAA compliant platform checks the compliance checkbox."	Configuration gaps are common. Compliance isn't guaranteed without oversight.

WHY IT MATTERS

Patient data doesn't just live in EHRs. It flows through inboxes, attachments, referrals, and care coordination chains every single day. If your email system isn't locked down, your HIPAA posture is a house of cards.

PAUBOX EMAIL SUITE

Send email as normal, but HIPAA compliant

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

Start for free

PAUBOX