Protecting Patients, Care Teams & Critical Communications

VOICE SECURITY

SUMMARY

The telephone is essential to healthcare, but it has also become an increasingly attractive target for cybercriminals.

What began as a nuisance has evolved into a serious security threat with real consequences for patients, care teams, and critical communications.

The Problem Has Greatly Evolved

The voice threat has changed.
What was once a productivity problem now includes deception, disruption, and attacks targeting enterprise systems.

The impact reaches across healthcare.
Malicious calls threaten patient trust, interrupt clinical workflows, and compromise essential communications.

Healthcare needs stronger defenses.
Protecting voice communications requires accountability, visibility, clear policies, and technical safeguards.

Why Healthcare?

Access
The real goal of most calls: a password reset, a way in

Six figures
What access to a corporate network can sell for on the dark web. Can start with a successful call to the help desk.

Data
What a stolen patient record is worth next to other stolen data

$250 to $310
For one complete patient record. A credit card goes for as little as $5. You can cancel a credit card but you can't cancel a medical

Leverage
Why hospitals end up paying

$6.64M
Average cost of a US healthcare breach, the highest of any industry. And a hospital can't go dark while it thinks about a response.

Sources: SOCRadar Dark Web Price Index 2026; IBM Cost of a Data Breach 2025

Areas of Impact

Patients
Attackers call patient rooms and impersonate billing departments, insurance representatives, or healthcare professionals. Patients recovering from procedures or under stress may be especially vulnerable.

Care Teams
Unwanted calls to nursing stations, emergency departments, and labor and delivery units interrupt clinical workflows and divert attention from patient care. In one example, a hospital's labor and delivery department received approximately 60 spoofed or unwanted calls daily.

Critical Comms
Attackers use high-volume calls to overwhelm switchboards and contact centers. They also target IT help desks, impersonating employees to reset passwords or gain unauthorized access. These attacks can disrupt operations and lead to broader incidents, including data theft and ransomware.

American Hospital Association™
Preferred Cybersecurity & Risk Service

mutare

mutare.com/voice-traffic-filter/