

Robocall Problem Resolved for Top Academic Medical Center



Patient Privacy Concerns and HIPAA Requirements Bolster Need for Voice Network Security

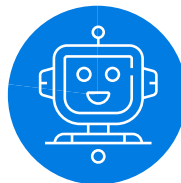
With scammers contacting patients in their hospital rooms to illicit their personal information via spoofed hospital numbers, one of the top academic medical centers in the US needed to protect its voice network not only to maintain the security of their operations and patients, but to comply with HIPAA requirements that protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The need for a managed service to protect not only their patients, but their long-standing reputation, became vital.

The voice channel is a crucial line of communication for hospitals and with hospitals becoming a more frequent target of robocall scams, protecting the voice channel is paramount. As one of the top-ranked academic medical centers in the country, the hospital not only had to protect the privacy of their patients, but their reputation too.

Business Challenge

The medical center and research institution was experiencing volumes of robocalls targeting direct dial-in numbers across its voice network system. HSS also wanted to mask calls from its outgoing phone numbers to protect patient privacy. With over 300 medical staff and 32,000 surgical procedures performed annually, as well as educating healthcare providers, the hospital couldn't risk scammers contacting their patients, their staff or their stakeholders. With HIPAA requirements, patient and staff safety and their reputation in both the academic and medical fields to maintain, the hospital needed to act quickly and partner with a telecommunications specialist to secure their voice network.

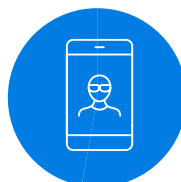
Scammers use machines to auto-dial numbers in patient rooms with pitches for products or ploys to steal a patient's personal information. If a spoofed call comes through a hospital's main phone line, staffers cannot distinguish it as fraudulent and ignore it. Since the number appears to be originating from inside the hospital, it could be coming from a patient in need of care. The scam often isn't uncovered until after someone has picked up the phone and exposed the patient to the robocall.



**Robocalls
& Spam**



**Harassing/Restricted
Calls**



**Spoofing &
Impersonation**

Solution

Suspect calls were blocked from connecting to the academic medical center's voice network. Not only did the reduction in robocalls improve response times for legitimate incoming calls, but the solution also reduced other types of fraudulent, harassing and threatening calls. The system was also able to mask the phone number of all the hospital's outgoing calls, in compliance with HIPAA requirements to protect patient privacy.

Outcome

Hospitals are increasingly becoming targets of robocall schemes, making them more vulnerable to fraud. Critically, an overwhelming volume of robocalls could potentially tie up a hospital's phone network, making it harder to communicate during an emergency and potentially exposing the hospital to liability.

Hospital voice security can become a question of life and death, especially during a crisis. The solution stops all fraudulent and malicious calls from connecting to the academic medical center's voice enterprise, freeing them to focus on healthy and positive patient outcomes.



TNS Enterprise Voice Security can help:



Detect and filter suspicious voice traffic



Deliver passive caller authentication through IVR integration



Support dynamic threat mitigation and policy enforcement



Improve inbound call answer rates and reduced wait times for customers.



Use metadata and behavioral analytics to evaluate caller legitimacy without disrupting legitimate interactions



Provide real-time insights and forensic call reporting

About TNS

Established more than 30 years ago, TNS has facilitated billions of branded calls, supporting thousands of organizations across more than 60 countries. TNS has over 10 years of call identification experience and handles over 1.5 billion daily call events from over 500 operators.



To learn how TNS Enterprise Voice Security can help your business, please contact our team.

solutions@tnsi.com
tnsi.com/solutions/communications/restoring-trust-to-voice/

