Strengthen Security + Trust in Your Healthcare Contact Center

Healthcare contact centers face rising fraud risks, while outdated authentication methods are time-consuming for patients and not as secure. While fraud affects payers, providers, and suppliers, AI-driven voice security solutions —such as voice-based authentication, ANI validation, and behavioral analysis—enhance fraud detection, streamline authentication, and can improve patient trust.

Rising fraud and low consumer satisfaction in healthcare

The healthcare industry has become the most targeted sector for data breaches. According to the National Library of Medicine, +41.2M in healthcare records were exposed in 2019 alone, and the US Department of Justice estimates that healthcare fraud may be costing the healthcare system $100B each year.[1]

Healthcare organizations are increasingly targeted by fraudsters, who exploit contact center vulnerabilities through methods like account reconnaissance, caller ID spoofing, and social engineering of agents. Traditional methods used by healthcare institutions to detect fraud, such as PINS, passwords, and security questions, are no longer sufficient.

Key takeaways:

- Use a risk-based approach to analyze calls for anomalies and catch more suspicious activity early.
- Voice security protocols enhance accuracy of patient identity verification, leading to more secure and efficient contact center experiences.
- Real time risk and fraud detection helps you stop fraud before it escalates.
- Improve customer experience by limiting the need for outdated authentication methods and increasing trust in your healthcare organization.

Statistics:

- The average cost of a healthcare data breach is $15M[2]
- Healthcare fraud may be costing the healthcare system $100B each year[2]
- 68% of all consumer interactions in the contact center still happen in the phone channel[3]

[1] U.S. Department of Justice. Criminal Resource Manual 976: Health Care Fraud—Generally. Last modified August 3, 2021.
[2] David M. Studdert, Alexander D. Wagner, and Michelle M. Mello, "Artificial Intelligence in Health Care: Anticipating Challenges to Ethics, Privacy, and Bias," Healthcare 8, no. 2 (June 2020): 133
[3] The 2024 US Contact Center Decision-Makers' Guide

©2025 Pindrop®. All rights reserved.

While stopping fraud is a priority, the healthcare sector has also lagged behind in consumer satisfaction. An NPS survey indicates that the medical sector has achieved just 70%[4] of the target net promoter score (NPS), which is behind the industry average of 81%. Healthcare organizations are struggling to keep up with patient satisfaction targets and the need for faster authentication while improving agent productivity and lowering contact center operational costs.

These issues highlight the need for more advanced, seamless fraud detection and authentication solutions. Luckily, AI-driven voice profiles, multifactor authentication, behavioral analysis, and patient identity verification tools can address healthcare security challenges and reduce fraud in the healthcare contact center.

Healthcare contact center security challenges

Fraud is a growing challenge in healthcare contact centers and occurs at various points in the supply chain. Fraudsters can target the organizations that pay for healthcare services (the payers), the individual and institutional providers of healthcare services like doctors, hospitals, and clinics, and the manufacturers and suppliers of medical equipment, devices, or supplies.

1. **Payers:** According to Gartner[6], improper claims payment and fraud contribute hundreds of billions of dollars to annual U.S. healthcare costs. However, few payers take steps to prevent this problem and instead rely on a reactive approach to fraud.
2. **Providers:** The emergence of telehealth services has opened up a new channel for potential fraud as healthcare organizations primarily focus on patient care and can inadvertently deprioritize security measures. Fraudsters may impersonate patients or their family members to obtain sensitive information such as Social Security numbers, Medicare numbers, or other personal data that can be used for identity theft[7].
3. **Manufacturers + suppliers:** Using social engineering schemes through the phone channel, a fraudster can deceive employees of companies at several human touch points throughout the healthcare supply chain to share confidential information. Once secured, this sensitive account data can be used to manipulate existing trading partner relationships to commit fraud.

[4] The 2024 US Contact Center Decision-Makers' Guide
[5] Gartner, Adopt Prospective Payment Integrity to Thwart Healthcare Fraud, 2023
[6] UHC, Know a health care scammer when you hear one, 2022

©2025 Pindrop®. All rights reserved.

Examples of healthcare fraud

Here are a few primary examples of fraud that take place in the healthcare supply chain:

1. **Prescription fraud:** Fraudsters perform account reconnaissance and account takeovers to steal large orders of prescription drugs, which can expose healthcare providers, pharmacies, and distributors to legal consequences, financial costs, and impact their reputation.
2. **Product recall fraud:** In this instance, a fraudster will call into a pharmacy acting as a manufacturer employee. Then, a courier is hired to pick up the shipment of the product that was supposedly recalled, and the product disappears.
3. **Payment fraud:** In this scenario, the fraudster calls into a pharmacy posing as a (legitimate) distributor employee, telling the pharmacy customer that payment terms have changed and to make payments to a new account, which is illegitimate and owned by the fraudster.
4. **Fraudulent ordering:** Involves a bad actor posing as a pharmacy employee placing an order from a distributor. The fraudster then hires a local courier to pick up the shipment, and deliver to a location that the fraudster specifies.

Healthcare fraud detection using voice security

Proper caller identification and authentication are paramount to addressing healthcare security challenges and improving the consumer experience. Voice security protocols like those below help identify and authenticate callers, enhance the caller experience, and provide diagnostic insights to reduce potential security threats in the contact center.

ANI validation and verification
With Automatic Number Identification (ANI), also known as Caller ID, each call is analyzed for threats and patterns to help determine whether it can be trusted.

Next-generation voice biometric authentication
When a new call enters the healthcare contact center, the caller's voice characteristics are analyzed, a risk-level is determined, and calls can be routed accordingly.

©2025 Pindrop®. All rights reserved.

Device analysis
Phoneprinting® Technology analyzes over 1,300 unique device and non-voice audio features using advanced AI and machine learning to create a distinct telephony profile that reveals geo-location, carrier, device type, and more. This enables healthcare contact centers to better verify customers' devices and catch repeat fraudsters.

Behavior analysis
Each healthcare customer has a unique interaction style. Behavioral analysis can classify the rhythm of keypresses to establish reliable human patterns. This process leads to better caller authentication and enables the contact center to detect more fraudulent behavior.

Risk and fraud analytics
Multifactor risk analytics can detect phone-based fraud in real time. Using advanced machine learning algorithms and acoustic and voice analysis, the system can identify high-risk calls and alert the contact center agent so they can stop fraud before it escalates.

Benefits of voice security

There are a myriad of benefits of implementing voice security for fraud detection in healthcare contact centers. For healthcare providers and insurers, voice security leads to faster and more secure patient authentication, which lowers fraud-related costs and risk. Faster verification can also lead to an increase in patient trust and customer satisfaction.

For patients, voice security eliminates the need to remember passwords or PINs, and helps to prevent identity theft through unauthorized account access. Voice security measures can also lead to faster and smoother provider interactions, increased trust, and higher customer satisfaction.

Take the next step toward healthcare fraud prevention

Incorporating voice security into your healthcare contact center can significantly enhance your ability to detect and mitigate fraud. Pindrop offers a seamless way to incorporate voice analysis and better secure your healthcare contact center. Explore our solutions page to learn about Pindrop® voice security technologies.

©2025 Pindrop®. All rights reserved.