Pindrop

Deepfake Readiness Checklist for Healthcare

Deepfakes and AI impersonations are making it harder to trust what you see and hear across everyday patient, member, and provider interactions. Identity needs to be verified continuously, not just once at the beginning of a call. This checklist breaks down the practical steps and components of shifting to continuous identity authentication.

1 Understand where your organization currently treats identity as a one-time check

Audit which real-time communication channels rely on static authentication (e.g., KBA, OTP, login). Identify the vulnerabilities and limitations of static authentication tools in these channels (e.g., using breached data to bypass KBA).

WHY?

Identity is increasingly assumed in live interactions when someone looks and sounds real and legacy authentication methods simply were not designed to defend against convincing voice and video deepfakes.

2 Extend continuous identity verification to workflows beyond traditional IAM boundaries

Common workflows targeted by voice and video deepfakes include:

- IT helpdesk and password reset workflows
- Remote clinical and IT hiring and onboarding
- Provider and prescriber interactions, including prior authorization and benefit verification lines
- Vendor and third-party interactions
- HSA/FSA account changes, claim payment workflow access

WHY?

Insider threats, fraudulent hires, and patient impersonations are rising due to weak identity verification in these flows. Pindrop data shows a 60x increase in AI-powered attacks per day.*

3 Validate location and session integrity in real time

Continuously monitor IP, geolocation, timezone mismatches, and VPN usage during sessions. Flag anomalies dynamically rather than relying on pre-session checks.

WHY?

Attackers increasingly use location obfuscation to bypass controls and impersonate trusted users.

4 Reduce authentication friction for participants

Deploy passive authentication that verifies voice, device, and behavior signals continuously across member services, patient access, pharmacy lines, etc. behind the scenes, without adding friction.

WHY?

Ruling out deepfakes is just one part of the equation. Organizations must validate right patient, member, or provider continuously, as well, while also preserving a good caller experience.

5 Align policies and trainings with AI-driven threat models

Update security policies to reflect:

- Deepfake-enabled impersonation of patients, providers, and staff
- AI-generated insider threats accessing clinical or administrative systems
- Help desk staff recognizing synthetic caller patterns before enabling credential resets

Ensure enforcement mechanisms match these realities. Update security awareness training to include deepfake threats.

WHY?

With social engineering and internal threats, it's imperative to inform employees of common signs of AI threats and train them on the tools they can use to catch them.

6 Surface real-time risk signals to users and security teams

Deploy visible, in-session security indicators (e.g., alerts, risk scores, participant analysis) that inform decision-making during interactions.

WHY?

Delayed detection is ineffective against fast-moving, AI-driven attacks occurring in live conversations. Humans detect AI-generated content only ~50% of the time.**

7 Deploy real-time deepfake detection across communication channels

Integrate tools, like Pindrop Pulse, that analyze audio and video streams live to detect synthetic media, voice cloning, and AI-generated personas. Focus on environments with high business impact: virtual staff meetings, member services calls, patient access lines, IT help desk calls, and other high-stakes interactions.

WHY?

AI-enabled fraud has surged by 1390% and is specifically targeting live interactions.***

Is your organization ready to withstand AI attacks?

Speak to a deepfake defense expert today.

*Based on Pindrop customer data analysis from Q1 2026 in comparison to the previous five quarters.
**Cooke et al., "As Good As A Coin Toss," 2025.
***Based on Pindrop customer data from Q4 2024-Q1 2026. Derived from a study of over 700M calls.

pindrop.com/healthcare | healthcare@pindrop.com