

WHITE PAPER

Streamlining patient verification in telemedicine: Reducing redundancy and enhancing trust



PRESENTED BY:

vouched

PUBLISHED BY:

FIERCE
Healthcare

Streamlining patient verification in telemedicine: Reducing redundancy and enhancing trust



Contents

Introduction3

The limitations of current patient verification practices3

The keys to effective digital patient verification.....4

A secure, seamless and compliant process 5

How compliance impacts patient verification strategies..... 6

Endnotes.....7

Introduction

While telemedicine leverages modern digital technology to connect patients to providers, the process of verifying a patient's identity remains largely analog and inefficient. Not only does this open the door to fraudulent behavior if practices do the bare minimum to manually verify identity and keep appointments on schedule. It also contributes to high abandonment rates as patients grow frustrated with a fragmented process that leads to delayed care or insurance reimbursement.

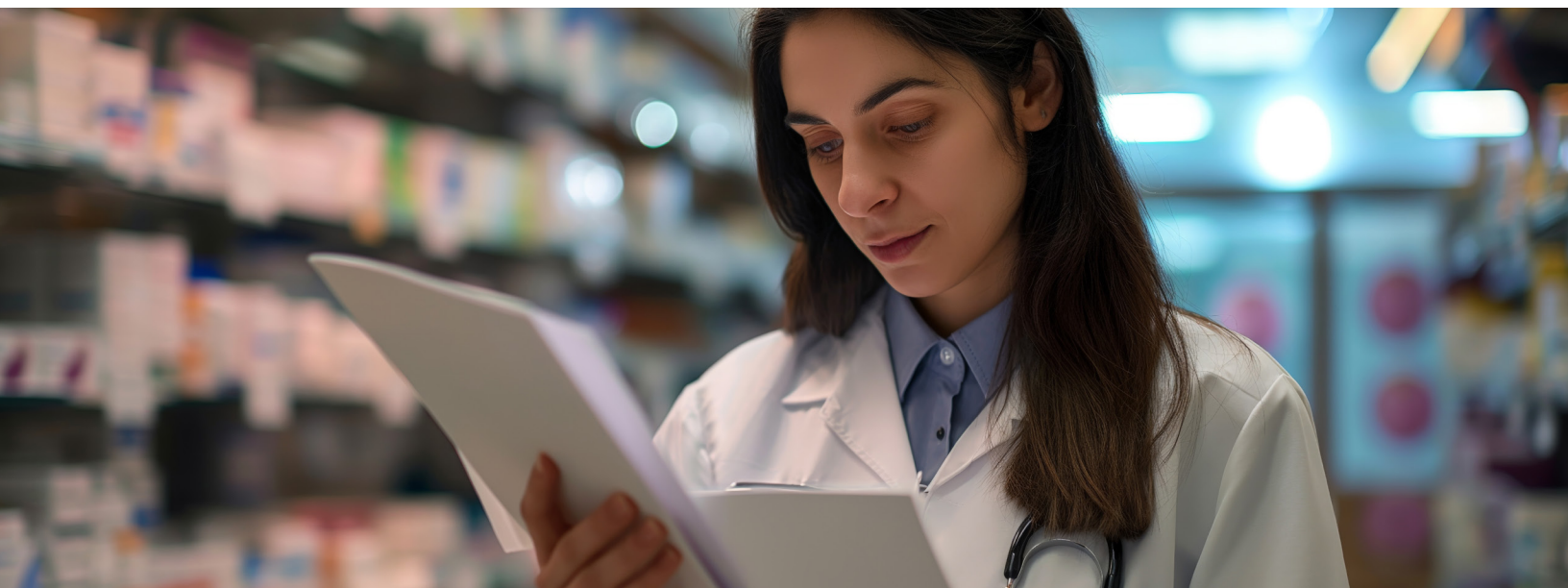
Digital patient verification marks an important step forward, but practices must be wary of requiring more work for patients to verify their identity or continually provide their information. The most effective workflows are based on the principles of Know Your Patient. KYP authenticates using multiple sources of personal and health information, including biometric data, to provide seamless and accurate authentication. Modern KYP practices also support automating and customizing verification workflows that reserve human checks for high-risk situations and streamline the process for low-risk encounters — contributing to a positive experience for clinical staff and patients alike.

The limitations of current patient verification practices

Telemedicine has made significant strides in enabling patients to access clinical care without visiting a brick-and-mortar healthcare facility. Patients who are too sick to travel, lack adequate transportation, or cannot miss a work shift can still receive much-needed care through their laptop or smartphone — and avoid care gaps that can lead to high-acuity episodes of care downstream.

Despite the technological advances that make telemedicine possible, verifying patient identity remains a primarily manual process. Best practice documentation from the Department of Health and Human Services suggests practitioners ask patients to show their valid photo ID to the camera¹ at the beginning of each telemedicine appointment² and any time medication is prescribed. Additional identify verification documents, as well as prior medical history, must be uploaded to a patient portal or typed into a Web form.

This process is time-consuming, redundant, transactional and insecure. A staff member within the physician practice must view and verify the patient's information manually. In the rush to keep an appointment on schedule, practices match the photo to the face but may not verify whether the name, phone number and address listed on a patient's documents actually match.



Digital verification workflows represent an important step forward, but they come with faults as well. While multifactor authentication is an accepted and familiar standard, a fragmented user experience can cause delays, especially when it comes to insurance verification. The ability to upload documents saves time and avoids data entry errors, but it keeps the onus on patients to do the legwork and contributes to delays as clinical staff review documents. The longer patients must wait, the more likely they are to abandon an appointment, with abandonment rates exceeding 60% all too common for telemedicine users.

Abandonment is far from the only consequence of getting patient verification wrong. A transactional process leads to redundant documentation; a patient seen seven times will have seven copies of their driver's license saved, for example. This gives practices more personally identifiable information (PII) and protected health information (PHI) to store — and increases the volume of valuable PII and PHI available to cyberattackers. In addition, practices that only verify a patient's name and face leave themselves open to fraudulent activity; underage patients could obtain medications intended for adults, while coordinated attacks could use false documents to obtain medications for illegal resale from dozens of telemedicine providers at the same time.

The keys to effective digital patient verification

The modern approach to digital patient verification is built on a foundation referred to as Know Your Patient (KYP). Like Know Your Customer in the financial sector, which defines how firms collect and verify identifying information about their customers, KYP principles dictate how practices should gather, authenticate and assess patient information.

KYP is a multi-step process. Entities must first collect information. This consists of demographic information consistent with KYC as well as medical history, biometric data and other relevant information the patient opts to share. From there, information must be cross-correlated. This step requires patient data the healthcare organization already has as well as information from a third-party database such as a credit bureau. Automated fraud checks are a must for each document that a clinic processes; the human eye cannot always detect whether a photo or signature has been manipulated, especially if it's being held up to a screen.



KYP is a multi-step process. Entities must first collect information. This consists of demographic information consistent with KYC as well as medical history, biometric data and other relevant information the patient opts to share.

A secure, seamless and compliant process

Done right, KYP brings security and efficiency to telehealth operations. Further augmenting KYP with artificial intelligence and machine learning allows practices to bring speed, precision and reliability to patient verification, all while refining the process over time as AI models evolve and improve. That positions practices to realize five key benefits of digital patient verification.

Real-time verification. Manually verifying patient information takes time and disrupts the workflow of a telemedicine visit — to the point that practices may do the bare minimum of solely matching names and faces. Using application programming interface (API) calls, digital patient verification solutions can analyze documents and confirm identity against additional data sources in real-time. This provides the high degree of security necessary for digital transactions in a seamless process that allows telemedicine appointments to proceed without interruption. That's an important feature for virtual urgent care visits, when time is of the essence, and for practices such as behavioral health or dermatology that may experience a high volume of virtual visits.

Pre-visit verification. For telemedicine appointments that patients have the option to schedule in advance, pre-visit verification offers patients the convenience of uploading their information on their own schedule. Not only does this eliminate the delays that come with verifying patient identity at the start of an appointment, but it also gives practices the opportunity to verify information at their convenience, as well as flag any documents that will require additional review prior to when an appointment has been scheduled. As noted, the latter use case can be valuable for verifying a patient's insurance coverage, which has traditionally been an onerous process.

Risk assessment. Certain telemedicine appointments come with a higher degree of risk than others. A patient's age, medical history or prior prescriptions can all increase the risk of fraudulent use or misuse of medication. In these scenarios, practices can escalate the verification process by requesting and verifying a patient's Social Security number or running a fraud check in the background as an appointment is happening. Along with reducing the risk of fraud and misuse in high-risk situations, effective risk assessment allows practices to avoid otherwise cumbersome identity verification steps for low-risk appointments, which improves the patient experience.



Automated patient onboarding. Identity verification can be a process fraught with friction. As the previous example described, requiring all patients to go through the same verification process is inconvenient for low-risk visits. It's also inconvenient for anyone with frequent telemedicine appointments, such as patients meeting with a dietician as part of a weight-loss care plan. Using AI to define and create custom verification workflows based on factors such as risk level, type of appointment and required data checks decreases this friction. Automated workflows also remove the guesswork from the verification process for practice staff as well as patients, making it both predictable and seamless.

Biometric verification. Digital patient verification is more than logging on for a scheduled appointment. Increasingly, patients need to access information after a visit, whether it's to review a visit summary or provide the forms necessary to obtain insurance reimbursement for a virtual visit. Practices can consider facial or fingerprint recognition capabilities to accurately verify patients who frequently access telemedicine services without the need to supply additional documentation or otherwise complete the verification process. Along with enhancing convenience and building trust with patients, this reduces the reliance on identity verification using PII and PHI that's attractive to attackers.

How compliance impacts patient verification strategies



The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) have set strict requirements for securing electronic protected health information (ePHI). Compliance means encrypting data at rest and in transit, restricting access to data based on users' roles and permissions, and tracking access of and modifications to data through audit trails. Any technology partner who handles ePHI as part of their relationship with a healthcare association must sign a Business Associate Agreement (BAA) outlining the steps it takes to protect patient data.

In addition, subsequent state and federal regulations have encouraged the secure exchange of ePHI to enhance care quality, reduce the utilization of unnecessary medical tests, and limit patient access to controlled substances. This applies to all practitioners, including those that provide telemedicine services. Given the central role ePHI plays in digital patient verification, no implementation strategy is complete without considering how data collection, verification, exchange, storage and destruction workflows must be structured to ensure regulatory compliance.

Choosing Vouched for digital ID verification

Digital identification plays an increasingly important role in our everyday lives. Facial and fingerprint recognition let users log into laptops or smartphones. Fifteen states, including California and New York, allow travelers to present a mobile driver's license at TSA checkpoints.³ Smartphone applications such as Apple Wallet, Google Wallet and Samsung Wallet, along with various third-party apps, let individuals manage their full identity profile in one place.

These emerging policy and technology trends address one of the most common challenges in identity verification. Requirements to frequently reset log-in passwords were once deemed a security best practice. However, these steps have become such a common cause of data breaches — through reuse of passwords, creation of weak passwords and so on — that cybersecurity experts now advise against them.⁴ Digital identity verification offers stronger means of authentication without the need for vulnerable user-generated passwords while keeping a human in the loop to oversee fraud checks when necessary.



Vouched provides patient verification solutions that bring together biometric analysis and data validation to help practices ensure patients checking into telemedicine appointments are, in fact, who they say they are. Along with its robust authentication features, Vouched provides workflow customization to automate and streamline the verification process. Vouched also integrates with leading telemedicine platforms, allowing practices to implement the solution quickly and realize ROI faster.

Healthcare organizations using Vouched have achieved significant business outcomes. Vouched provides patient verification in under 10 seconds with a 97% success rate and an accuracy rate of more than 99.5%. This reduced the reliance on manual verification efforts and increased clinical staff's capacity to focus on patient care. One customer saw automation boost conversion rates for new patient onboarding from 40% to 95%, success that contributed millions of dollars in additional annual revenue.⁵

As practices and patients increasingly embrace telemedicine as a convenient and cost-effective way to increase access to care, it's imperative that patient verification evolve beyond manual workflows. Digital identity verification streamlines the process with speed and accuracy, reserving human checks for high-risk appointments and enabling automated verification for the most common scenarios to improve the experience for patients and clinicians alike. Learn more about how Vouched brings digital identity verification to healthcare or request a demo of our solution in action.

Endnotes

- 1 [Telehealth for Providers: What You Need to Know](#). U.S. Department of Health and Human Services. Revised October 2024.
- 2 [Telehealth for behavioral health care](#). HHS. October 2024.
- 3 [Participating States and Eligible Digital IDs](#). Transportation Security Administration. March 2025.
- 4 [The problems with forcing regular password expiry](#). National Cyber Security Centre. October 2016.
- 5 [Streamlined Onboarding and Secure Betting with Vouched ID Verification KYC Solution](#). Vouched. April 2025.

vouched

Vouched is a leading AI-powered identity verification platform serving industries with high-stakes verification needs like healthcare, finance, and automotive. Trusted by enterprises around the world, Vouched verifies millions of identities annually with speed, accuracy, and compliance.

To learn more, visit www.vouched.id. To schedule a demo, click here.

