JUNE/JULY 2021

FUTURE of IDENTITY Report

PYMNTS.com | AUTOTIX IDENTITY INTELLIGENCE

FUTURE of IDENTITY Report

ACKNOWLEDGMENT

The Future Of Identity Report was done in collaboration with AU10TIX, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

PYMNTS.com | AU10TIX IDENTITY INTELLIGENCE

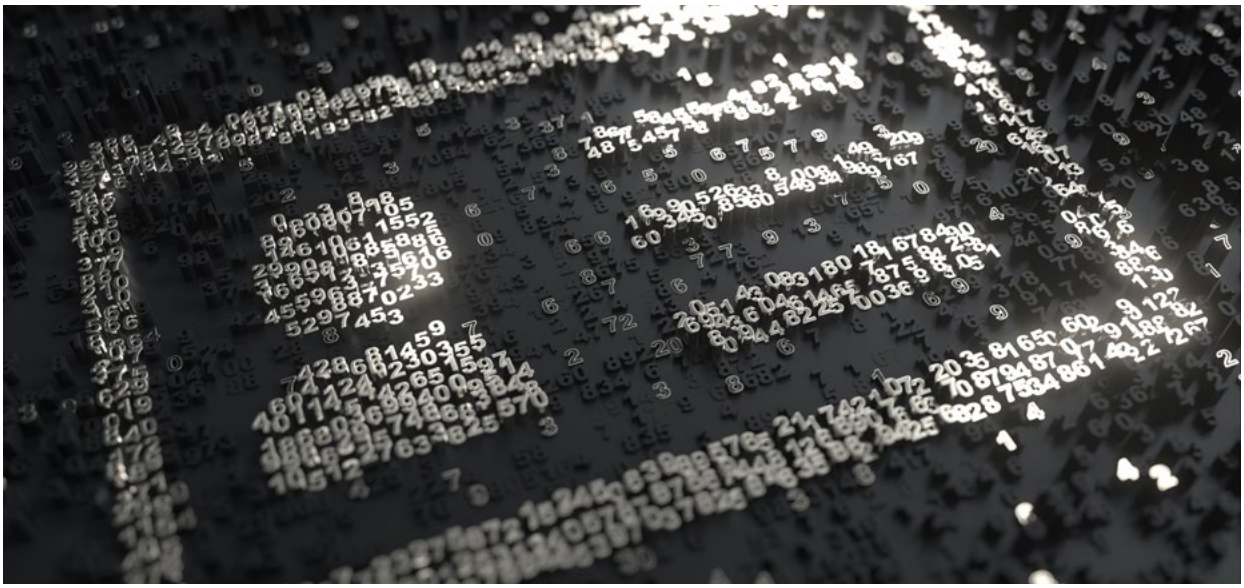
TABLE OF CONTENTS

WHAT'S INSIDE

Healthcare has gone digital alongside most other industries, with telehealth and other virtual medical solutions gaining popularity in the wake of stay-at-home and social distancing mandates. Virtual services' usage has fallen somewhat in recent months as vaccination rates rise in the United States, but there are indications that digital health will continue to occupy a critical role in the space over the next several years. Digital health funding reached $9 billion in Q1 2021, for example. Many healthcare professionals have also pointed to telehealth's unique benefits for behavioral and mental health appointments as well as its usefulness when sending documentation to patients.

Healthcare providers must be prepared to address patients' new needs and preferences relating to data privacy and payments as the virtual healthcare space continues to develop. Consumers now seek swifter digital payment methods when making insurance claims or paying medical bills. Almost half of individuals in one recent survey stated that healthcare was the most difficult industry in which to make payments, for example. Consumers' desire for swifter payments is rising in parallel with their concerns for privacy and security as fraudsters and cybercriminals more heavily target the online healthcare space. Sensitive patient data remains highly valuable within the black market, with 2017 data finding that such information can be 20 to 50 times more valuable than financial data. These fraudsters are targeting healthcare companies to gain such data for future malicious means, with one 2020 study reporting that 57 percent of U.S. healthcare providers had experienced phishing attacks in the past 12 months.

Cybercriminals' emboldened strikes are making incorporating robust identity verification measures crucial for healthcare providers, especially because failing to provide stringent



security could strain patient relationships. Recent PYMNTS data found that 38 percent of consumers are "very" or "extremely" concerned about the security of their healthcare accounts. Sixty-two percent indicated that they would be willing to spend more time going through the digital identity verification process when opening healthcare accounts for greater security.

Verifying the identities of doctors or other healthcare providers is also becoming more important, as fraudsters are tapping stolen credentials to impersonate medical insurance providers, healthcare officials or other employees in the space. Twenty-one percent of healthcare providers **experienced** credential-harvesting attacks — including patient and other protected data — within a 12-month period, for example. The U.S. Better Business Bureau **issued** warnings against phone scams in which fraudsters pretend to be "healthcare benefits advocates" attempting to phish for users' Medicare or Medicaid identity numbers. Innovating digital identity verification solutions as well as creating a sense of trust for all parties involved should be a priority for healthcare providers given such developments, especially as the rising interest in telehealth services attracts more fraudsters.

AROUND THE IDENTITY VERIFICATION SPACE

Healthcare-related data breaches and fraud can have long-lasting consequences. Fraudsters can utilize customers' private details to launch phishing schemes or create synthetic identities for additional scams, for example. A recent CVS Health breach **exposed** 1 billion search records, for example, including customers' user IDs, email addresses and the queries they entered on the pharmacy's website. The database in which such records were stored reportedly failed to require authentication, leaving it unprotected against bad actors. Incorporating digital identity verification solutions that can distinguish between legitimate customers and fraudsters leveraging synthetic identities is

becoming increasingly important for healthcare providers.

Data breaches and other cybercrimes are likely to become pressing concerns for the healthcare industry as more consumers interact with and pay their medical professionals digitally. Individuals have become more comfortable with telehealth services that utilize video, text and other virtual features over the past year, and many in the industry anticipate this trend to have staying power. Forty-three percent of Americans **indicated** that they want to continue using telehealth services in the near future, for example, and 45 percent believe virtual services afford them the same quality of care as in-person healthcare visits.

Consumers' growing ease with digital healthcare services is also having a notable impact on their payment preferences. More patients now wish to pay their medical bills digitally, with approximately two-thirds of those who used telehealth solutions last year **stating** that they preferred "safer" and "cleaner" ways to pay for them. The availability of digital payment methods such as mobile wallets and online payment portals is still relatively limited, however. Approximately half of all patients continue to receive their medical bills via postal mail, with just 28 percent saying that they could pay their bills using online portals.

For more on these stories and other identity verification headlines, read the Report's News and Trends section (p. 12).

WHY AI IS CRITICAL FOR DIGITAL IDENTITY VERIFICATION IN THE TELEHEALTH AGE

Healthcare providers significantly shifted the ways they interacted with patients to provide needed care over the past year, but siloed data and increased patient privacy concerns created severe difficulties in doing so successfully. Patients now expect to be able to connect with their providers wherever they are, including on digital channels, putting pressure on healthcare services to not only provide seamless online experiences but to do so securely. In this month's Feature Story (p. 9), Adam Silverman, M.D., chief medical officer for healthcare artificial intelligence (AI) service **Syllable** and Vig Chandramouli, principal of healthcare at FinTech and healthcare venture capital firm **Oak HC/FT**, discuss why healthcare providers must rethink the way they treat data and conduct digital identity verification to meet both shifting security and patient care needs — and detail how technologies like AI help.

DEEP DIVE: WHY INCORPORATING CONTACTLESS PAYMENTS AND BIOMETRIC VERIFICATION MEASURES IS CRITICAL FOR HEALTHCARE PROVIDERS

More patients began tapping telehealth services over the past year, and this trend carries on even as brick-and-mortar locations reopen. This has presented challenges for healthcare providers, which must offer digital-first solutions that allow consumers to interact swiftly and conveniently with providers without sacrificing security and quality. This month's Deep Dive (p. 16) examines the healthcare space's ongoing digital shifts and details why medical providers should adopt contactless payments and biometric verification solutions to create frictionless and secure patient experiences.

EXECUTIVE INSIGHT

How have digital identity verification needs changed for healthcare companies in the past year as more consumers turned to telehealth and other online services for their medical needs?

"With surging demand for remote [or] telehealth medical services, there is a growing need to digitally identify and authenticate patients to ensure that patient care is provided to and by the right person, [that] documents and medical info are accurately associated with that person [and that] fraud is eliminated from the payment process and medical credentials are not stolen.

In these situations, it is not enough to answer common security questions, such as your favorite vacation or first car, to verify who you are. Similarly, when uploading documents, it is important that there are no mistakes, as even one error could be costly.

As such, the healthcare industry, alongside other digital transformation [players], is pushing identity verification into the mainstream to increase convenience and improve patient experiences while confidently managing out risk.

In five to 10 years, consumers will manage their health, call for a service [and] not a specific provider and expect [that] their information is not just in one place, but securely distributed and connected."

How can healthcare providers ensure that their patients' medical, financial and personal data is secure? What technologies and solutions are key to achieving this?

"While the financial services sector has been fighting cybercrime for years, healthcare is just getting started; with the rise of digital healthcare, there is an infrastructure and knowledge gap to close.

Consider the correlation between fraud, payments and insurance in healthcare. How is it that you can go to a provider, receive service, pay and months later get charged for a service never provided? To address this issue — and more serious ones like the wrong prescription, service or record sharing — organizations need to leverage automated verification solutions that secure identities, validate procedures and eliminate fraud.

For remote cases, digital solutions that capture, verify and validate ID documents or a person's presence and credentials are key. For in-person [situations], there is an opportunity to combine these tools with a biometric strip or [a one-to-one] safeguard so that, as a patient moves through their experience, providers can continuously confirm identities and medical data. This is important for compliance and confidentiality."

How do you see the role of tools such as biometrics and voice recognition for identification growing within the healthcare space as telehealth usage continues?

"Identity verification is a critical security piece in telehealth, and voice recognition provides a great automation layer to identity, but [using one tool] alone is not good enough. Layers are critical.

When a legitimate patient is trying to gain access to an account, make a transaction or receive care, they need a seamless, frictionless consumer experience that recognizes them, verifies their care provider and blocks fraudsters out.

By starting with a government-issued ID [such as a] passport or driver's license, then combining it with other available information about the user — [including their] medical certificate, previous patient record, facial recognition, fingerprints [or] voice — we can accurately verify if the person providing or receiving the service along the process is indeed who they say they are.

The future of identity in healthcare centers on the ability to quickly read, protect and correlate personal data; it hinges on building a platform with dynamic capabilities that accounts for this and leverages multiple identity verification methods."

ASHER POLANI
Executive advisor, healthcare
AU10TIX

FIVE FAST FACTS

IDENTITY THEFT

21 percent of healthcare firms experienced credential-stealing attacks within a 12-month period.

DATA BREACHES

Data breaches expanded by 55 percent in the healthcare sector between 2019 and 2020.

PRIVACY CONCERNS

54 percent of consumers are concerned about security when accessing personal data online.

TOUCHLESS PAYMENTS

58 percent of patients have favorable opinions of touchless payment options.

BIOMETRICS

54 percent of Americans identified biometrics as their top choice for healthcare record identification.

FEATURE STORY

How AI And Digital Identity Verification Can Secure The Telehealth Age

The healthcare industry experienced sweeping changes in 2020 as medical providers worked on overdrive to fulfill the needs of both patients visiting physical hospitals or clinics and those tapping telehealth services in unprecedented numbers. One of the challenges with serving patients effectively online is that many healthcare providers store sensitive personal and medical information in electronic medical record (EMR) systems that are often inoperable with each other. This creates friction when attempting to provide care for patients swiftly and conveniently and also when keeping that information secure, said Adam Silverman, M.D., chief medical officer for healthcare AI service **Syllable**.

"What we saw on our end were huge numbers of patients who struggled with [using authentication portals to access telehealth], so, [though the portals were] put in place to ensure privacy, [consumers were] running headlong into this issue, [which was] creating an obstacle to care," Silverman explained. "Health systems now were not only being inundated with people calling to schedule a video consultation, but ... they were being flooded on their IT help desks by the same patients who could not log in to the portal in order to obtain care, and so it sort of reinforced this constant struggle between privacy on one hand and access or interoperability on the other."

PYMNTS spoke with both Silverman and Vig Chandramouli, principal of healthcare at FinTech and healthcare venture capital firm

Oak HC/FT, to determine how the events of 2020 have impacted providers' patient care and digital identity verification needs. Serving patients effectively across multiple channels as more expect to connect in a variety of in-person and digital ways with their healthcare services is essential for the industry, and providers must also ensure they are adjusting their cybersecurity strategies accordingly.

INNOVATING AND UNIFYING IDENTITY IN A DIGITAL-FIRST HEALTHCARE WORLD

Healthcare providers are already aware of the need to innovate to match patients' strengthening preferences for digital healthcare and the need for enhanced security in this channel. EMR systems can be decades old and were designed to protect patients' privacy when they were initially rolled out in the mid-2000s, Silverman said. The issue now is that healthcare systems have yet to evolve beyond those legacy expectations, relying on "castle and moat" strategies for protecting patients' data — so long as no medical information leaks out of the system, it is viewed as secure, he said. This approach is no longer viable in a world in which fraudsters are targeting digital systems, however — and one in which patients are increasingly aware of that fact, according to Chandramouli.

"Every day in the news, you now read about some ransomware attack or cybercrime or see how some pipeline is shut down or some hospital was held hostage, and these are all very possible and increasingly more likely things going forward," said Chandramouli. "But I think that what that distills down into for the average consumer is just being worried generally about, 'What data am I submitting and to where and to whom? I have no idea where this data goes next.'"

Ensuring sensitive personal information cannot be moved outside of healthcare systems by disgruntled or malicious employees is just as critical to security as ensuring medical data is safe during patient intake, Chandramouli continued. This means chief security officers, who typically think of cybersecurity in terms

of the system and not in terms of the patients, according to Silverman, must adjust their strategies to protect patient data first in a way that can help foster trust. This means shifting away from digital identification measures such as usernames and passwords that have become more frustrating and less secure in favor of solutions that utilize more advanced technologies.

"I think if we found a passwordless option for patients, … that would certainly improve their experience," Silverman said. "It probably would be less expensive, because people would stop calling the IT help desk, and those calls take 20 to 30 minutes to try to complete and help somebody change the password. I think [login innovation] is a win-win for everybody."

Utilizing tools such as biometrics that rely on harder-to-fake patient identifiers, including behavioral indicators that they are in the same place as the device they are using to speak with providers, is one way healthcare services can boost their identification measures. Technologies such as AI are also set to play a larger role within the healthcare space for the future of digital identity verification as the demand for more robust solutions intensifies.

TAKING A PAGE FROM THE RETAIL AND PAYMENTS AI PLAYBOOKS

Incorporating AI could have massive benefits for providers both in terms of securing patients' data and allowing them to create the seamless user experiences patients demand, Silverman explained. Healthcare providers should therefore examine the way other industries, notably the retail or digital payments spaces, have utilized AI or other automated tools for such purposes.

"I think, on the back end … is where I think a lot of the really exciting stuff can get done, because that is where AI really can be very beneficial in terms of monitoring the networks and identifying signals or patterns that are abnormal for a given persona," Silverman said. "If you think about it, 10, 15 years ago if you traveled outside of your home ZIP code, [if] you went on vacation, Visa would call you and say, 'We just saw you filled up your gas tank in the neighboring state' and they would say, 'Are you traveling, because we just got a charge.' So they have even gotten more sophisticated in terms of their signal processing and [their] use of artificial intelligence to identify fraud. Healthcare [companies] should be able to do the same thing."

Using the payments space as a blueprint could be key for healthcare providers to stay competitive as digital healthcare becomes more popular and as digital fraud becomes more prevalent. Bridging the divide between privacy and convenience, physical and digital, access and security or even between one database and another is the future of identity in healthcare and where automation, machine learning and collaboration can make a real impact.

NEWS & TRENDS

Healthcare identification developments

CONSUMERS REPORT INCREASED CONCERNS OVER HEALTH DATA SECURITY

Individuals are heavily invested in keeping their medical data private and secure, and many are becoming more concerned over their providers' actions regarding personal data. Twenty-seven percent of individuals in one survey reported that they would switch healthcare providers if their current organizations suffered data breaches, for example. Reports also show that bad actors are targeting healthcare providers with increasing frequency, as medical data breaches have affected more than 250 million consumers between 2005 and 2019. The events of the past year exacerbated this trend: The number of medical-related data breaches surged by 55 percent between 2019 and 2020.

Stolen data in healthcare can have a ripple effect throughout consumers' overall information security and their financial health, making the protection of medical information critical. Healthcare providers will have to vigorously protect their platforms from data breaches and other cyberattacks to gain and keep their patients' trust. This will be particularly important as digitally savvy consumers continue to monitor their data privacy and keep track of how companies or providers are authenticating access to their personal information.

CVS HEALTH ATTACK LEAVES 1 BILLION SEARCH RECORDS EXPOSED

Healthcare-related data breaches are growing in both scale and frequency, making it essential for providers to offer digital verification solutions that can distinguish between legitimate users and fraudsters leveraging synthetic identities. A CVS Health breach that occurred earlier this year exposed 1 billion stored search records to malicious actors, for example. The database did not require any form of authentication for access, according to the report, making it vulnerable to unauthorized access. The compromised personal information included user IDs, email addresses and consumers' vaccine- and medication-related search queries on the pharmacy's website. The incident highlights just how critical it is for healthcare providers to utilize verification measures that can safeguard customers' details and ensure access is granted only to legitimate individuals.

LAS VEGAS UNIVERSITY MEDICAL CENTER SUFFERS DATA BREACH

Such data breaches can have lasting consequences for patients, inviting instances of future fraud and identity theft as criminals tap stolen credentials to craft synthetic identities. These breaches are also becoming more common. Las Vegas-based healthcare entity University Medical Center recently reported an attack in which cybercriminals broke into a data center storing personal patient information, such as Social Security numbers, driver's licenses and passports. These details were then posted on the University Medical Center website. The hospital is notifying patients that their information could be at risk and is also offering complimentary identity and credit monitoring services, according to recent statements. Such offers do not erase the potential harm that fraudsters could cause when using these stolen details

to impersonate patients and perpetuate further scams, however.

TELEHEALTH SERVICES CONTINUE TO EXPERIENCE INCREASED USAGE

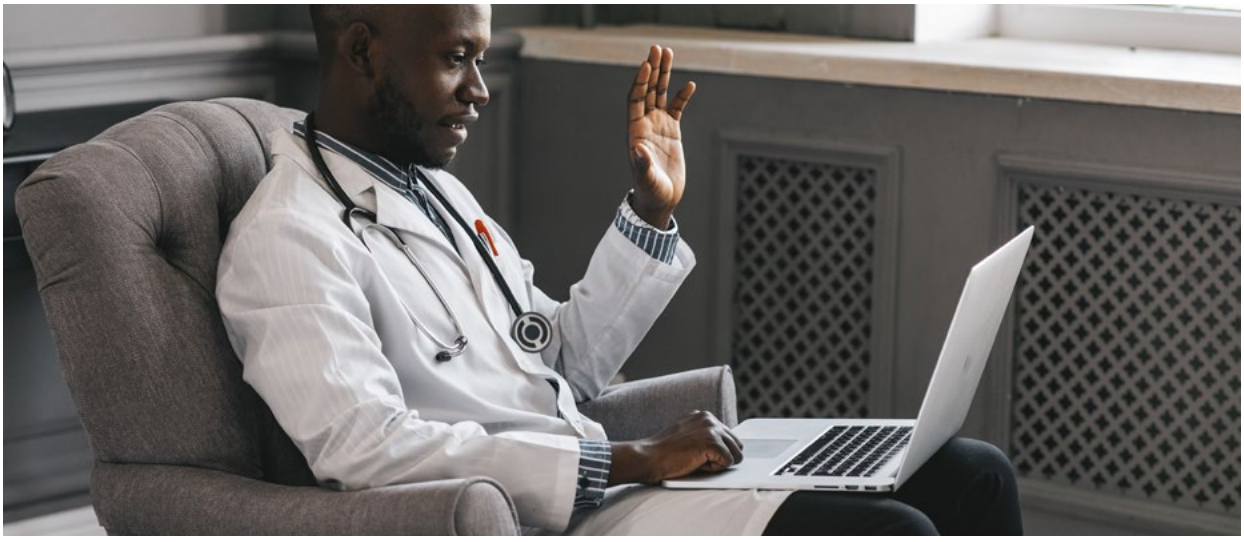
Stopping cyberattacks and fraud will remain a top concern in the healthcare industry, especially as more consumers interact with their providers via digital channels and need to verify that the providers they see digitally are who they say they are and hold necessary credentials. Telehealth solutions that enable patients to touch base with medical providers via video or other digital tools experienced a boom in adoption in 2020 that appears to be long-lasting. Telehealth visits exploded 154 percent between March 2019 and March 2020, for example. One recent study from the American Psychiatric Association found that 43 percent of patients want to continue using telehealth services in the future, and 34 percent would rather schedule telehealth appointments than visit medical professionals in person.

The virtual healthcare space will likely expand over the next few years given such trends. Forty-five percent of consumers believe telehealth visits afford them the same quality of care as in-person ones. Creating a seamless and secure experience online is thus critical for healthcare providers.

Digital payments and identity in healthcare

PATIENTS PREFER TAPPING CONTACTLESS PAYMENT METHODS FOR HEALTHCARE BILLS

More patients are also looking to use digital and contactless methods to pay for their medical costs, according to another report,



which found that roughly two-thirds of U.S. consumers reported using telehealth providers in 2020 and that nearly half preferred "safer" and "cleaner" ways to pay their bills, such as mobile wallets and online payment portals.

Consumers' growing fondness for digital payment methods should make them a key focal point for healthcare providers, but mobile and contactless payment methods' security measures can sometimes fall short of those used to secure other payment forms. Implementing security tools such as biometrics that are inherently mobile is one way that providers improve such payment methods' security.

Emerging digital identity trends

CONSUMERS CONSIDER PROTECTIVE SOLUTIONS AS IDENTITY THEFT RISES

Identity theft became an even more dangerous threat both to healthcare providers and patients in 2020. One study found that the number of U.S. adults claiming their identities were stolen rose 67 percent between 2019 and last year, meaning identity theft or related scams affected approximately 21 million individuals. This increase has led many consumers to contemplate technologies that can safeguard their personal information, and 20 percent of Americans are planning to purchase some form of identity theft protection within the next year.

The identity monitoring industry in general is expected to experience an increase of more than $4 billion in revenue by 2022. This shows that consumers are becoming more cognizant of and invested in protecting their digital identities, meaning online providers in all industries must work to keep their information safe and secure.

REMOTE ONBOARDING EXPANSION PROMPTS DIGITAL IDENTIFICATION SPEND

More individuals are also finding new healthcare providers, banks and merchants via digital channels, spotlighting the importance of seamless digital onboarding and login processes. Protecting these digital interactions from fraudsters as well as boosting users' confidence in their overall security is a crucial consideration for businesses, and spending on digital identity verification solutions is expected to grow 77 percent by 2026 to about $16.7 billion. Companies are expected to spend $9.4 billion on such solutions in 2021.

Merchants must take care to integrate digital verification tools that do not add unnecessary friction into the onboarding process. Ensuring that the security measures attached to their onboarding processes are as seamless as possible should be a top goal for merchants across the globe as they further digitize their services and operations.

DEEP DIVE

How Biometrics And Contactless Payments Are Key To Creating Patient-First Healthcare Experiences

The healthcare industry's rapid changes over the past year required providers to adjust to new operations at their in-person facilities as well as cope with surges in visitors accessing their services digitally. Telehealth visits rose rapidly during the global health crisis's early months, accounting for 13 percent of private medical claims in April 2020 compared to the less than 1 percent they accounted for in January of that year. PYMNTS data also found that consumers' demands for digital healthcare experiences were 50 to 175 times greater at the start of the health crisis than they were before it. Virtual visits have declined since their April 2020 peak, but telehealth services are still experiencing increased adoption compared to their 2019 rates.

The digital healthcare migration has created some significant challenges for healthcare providers. They must ensure that their patients' virtual experiences offer the speed, quality and privacy that puts them on a par with in-person visits, and many customers are beginning to ask their healthcare providers to support digital payment methods, such as contactless credit and debit card payments. Consumers are also expressing more concerns regarding online privacy and these

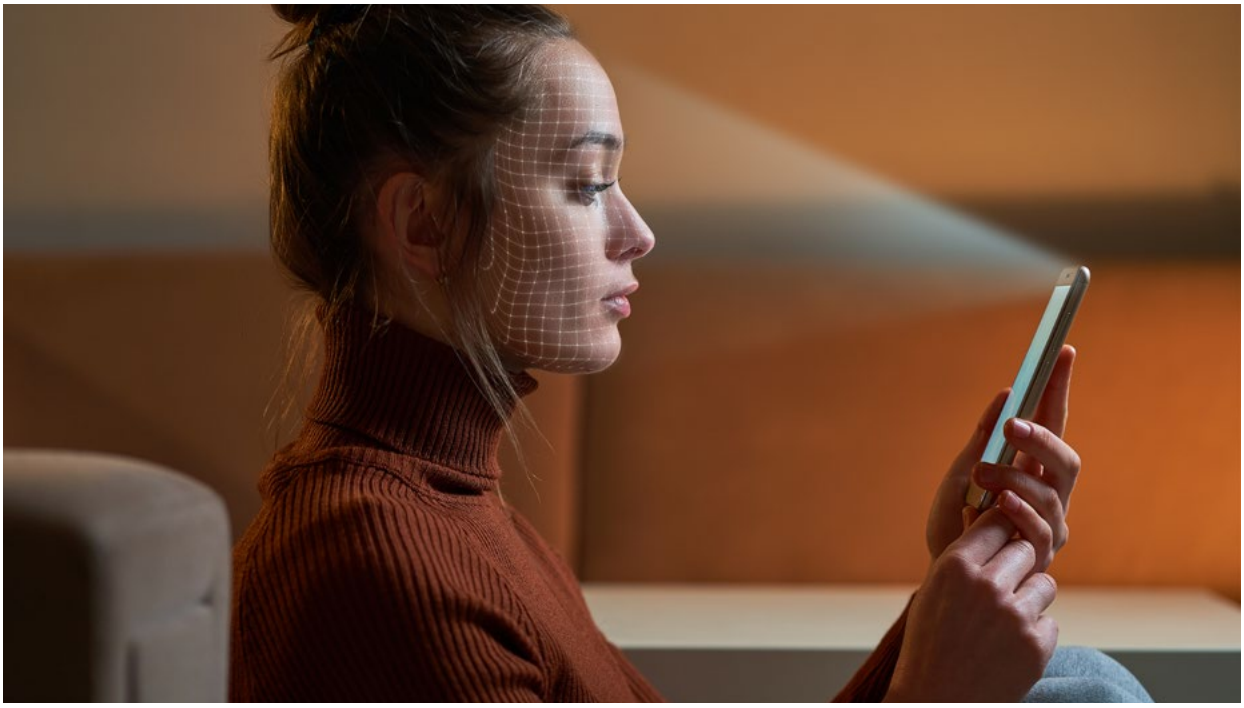
digital health services' security. One recent study found that 54 percent of patients cited concerns regarding cybersecurity when accessing their personally identifiable information (PII) online, for example.

Digital verification and reverification solutions must be a component of healthcare providers' new digital channels and services to ease patients' concerns, as failing to do so could severely impact consumers' trust in their providers, yet these solutions must also not add undue friction. The following Deep Dive will analyze emerging trends and developments within the broader healthcare industry as well as examine how digital shifts are affecting identity verification and payment needs within the space. It will also explore why supporting robust digital identification solutions and innovative payments in a personalized way is a necessary part of providing the patient-centric experiences consumers crave.

SHIFTING TELEHEALTH PAYMENT PREFERENCES AND SECURITY NEEDS

Consumers' interest in telehealth services has been on the rise for several years, but the global health crisis played a large role in prompting healthcare providers to support virtual services. One October 2020 study found that the portion of physicians who used telehealth to connect with patients had increased fourfold since 2019, for example.

Healthcare providers and medical professionals must overcome a steep learning curve as they build out these digital-first health solutions, however, which includes responding



quickly to patients' new expectations for interactions and transactions. Consumers are putting more stock in accessing smoother healthcare payments, as more than half of patients are willing to contemplate switching providers if doing so granted improved payment experiences. More patients are looking for mobile-optimized payment solutions as well, with 31 percent of customers claiming that they pay their medical bills faster when they can do so via mobile app.

Consumers are also seeking swift payment methods that can be used for both virtual and in-person visits, prompting more interest in contactless solutions. These trends signify that healthcare providers must prioritize offering digital-first payment methods and telehealth services to meet patients' new expectations. Successfully operating in a digital-first healthcare space requires putting cutting-edge verification solutions and security measures in place, however. The need for more stringent security methods is intensifying as the healthcare space — especially the virtual healthcare arena — becomes of higher interest to fraudsters, stoking fears of medical identity theft that could also financially impact patients. Fraudsters utilizing stolen credentials could impersonate patients to file false insurance claims, for example, defrauding the patient, the healthcare provider and the insurer all at once. Implementing identity verification solutions that can block such schemes and easily distinguish between legitimate consumers and fraudsters armed with synthetic identities is thus critical.

PRIVACY PREFERENCES IN THE VIRTUAL HEALTH WORLD

The events of the past year have illuminated healthcare providers' evolving security needs. Fraudsters are increasingly targeting the space as services move online and as consumers' privacy and security preferences change — and bad actors have been quick to take advantage of these shifts. Data breaches now cost healthcare providers $7.1 million per incident on average — the highest average cost observed for any industry. Lost PII also costs an average of $150 per individual record regardless of industry, which means recovering from such breaches is becoming an expensive endeavor for companies of all types.

Medical data theft can be particularly devastating for providers and patients, especially as the former must comply with the Health Insurance Portability and Accountability Act and other regulatory requirements about storing sensitive information. Data breaches that allow fraudsters to access such information could violate these rules and enable bad actors to create synthetic identities and launch other fraud schemes.

Medical entities can also lose patients' trust if they fail to keep their data safe. Customers' expectations for online privacy and security are rising alongside their expectations for better access to digital healthcare services. The portion of consumers who would abandon their healthcare providers for new services in the event of a cyberattack swelled 30 percent between 2019 and 2020, for example, and the majority of consumers are

reporting concerns about security when they log in and view their PII online with their healthcare providers. Consumers want to be sure that their providers are keeping this log-in process safe from fraudsters, protecting gateways such as patient portals, for example. Forty-six percent of providers noted that securing such portals can be challenging when patients also expect the login process to be seamless. Figuring out how to balance those two components represents a critical task for providers as the healthcare space further digitizes.

THE FUTURE OF IDENTITY VERIFICATION IN HEALTHCARE

Healthcare providers can tap a varied list of emerging technologies and solutions, including biometrics, liveness detection or automated data comparisons, to verify patients' identities and keep their virtual platforms safe. Consumers' growing mobile-centric tendencies make biometrics an enticing option. Many smartphones enable biometric solutions such as facial or fingerprint recognition, which could grant enhanced security to healthcare providers rolling out more digital services. One study found that 54 percent of Americans chose biometrics as their top choice for healthcare record identification — a fact that speaks to consumers' comfort with using such verification methods.

Integrating biometrics into telehealth services and healthcare payments for stronger verification presents numerous possibilities for healthcare providers, allowing them to implement higher security and more robust credentialing services while also championing

personalization and ease of use for consumers. These concepts are becoming more common in the healthcare industry as virtual care expands, indicating that providers are aware of the need for identification innovation. The presence of digital identities unique to each individual's biometric signature may remain a point of interest within the healthcare space for the next few years as security needs shift. The healthcare industry is going through a period of rapid digital innovation, and providers will have to keep their eyes on digital identity trends and challenges to ensure they are keeping both themselves and their customers safe.

ABOUT

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

AU10TIX
IDENTITY INTELLIGENCE

AU10TIX is an identity intelligence company on a mission to obliterate fraud and make the world a more secure, inclusive place through automated technologies that confidently link physical and digital identities. Our global, modular solutions — from identity document verification to biometric authentication, liveness detection and synthetic fraud detection — are backed by four decades of experience and enable businesses and customers to confidently connect.

FUTURE of IDENTITY Report

DISCLAIMER

The Future Of Identity Report may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED" "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.