Daon®

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

Introduction 3

Challenges Facing the Healthcare Industry 4

- Supply and demand pressures 4
- Cost barriers 4
- An aging U.S. population 4
- Rising rates of chronic disease 5
- Shortages of healthcare professionals 5

Regulatory Pressures 6

HIPAA (1996) 6

GDPR (2018) 7

Cybersecurity concerns 8

FHIR Protocol 9

Tools Needed for the Next Generation of Healthcare Providers 10

Hospitals 10

Pharmacies 10

Labs 11

Independent providers 11

Insurance companies 12

Utilizing Identity Proofing Solutions in Healthcare Organizations 13

Better protect patient health records 14

Remove accessibility barriers for online access 14

Authenticate patient identities remotely 14

Improve healthcare equity 15

Simplify processes 15

Allow physicians to write prescriptions online - securely 15

Onboard remote healthcare employees 15

Onboard users 15

Benefits of Identity and Access Management (IAM) 16

Internal workflow optimization 16

Compliance and security 16

System integration 16

Cost reduction and efficiency 16

Easier patient journeys 16

Improved patient care outcomes 16

Your Identity Proofing & Authentication Partner of Choice 17

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

The software underlying healthcare mobile applications is sophisticated in both its security and the user experience it offers customers. Today's apps are designed to simultaneously provide a seamless, low-friction interface for users while maintaining healthcare privacy, a critical concern for both providers and patients. This delicate balance between ease and security keeps organizations on their toes, and the challenge is compounded by increasing cyberattacks targeting sensitive patient information.

The high costs involved in developing and maintaining apps and the systems that run them come at a high price, and that price falls squarely upon the healthcare organizations themselves. When those systems fail to deliver, healthcare organizations can fall victim to identity breaches that, on average, cost as much as $8 million. Meanwhile, government-imposed penalties due to these breaches can also amount to millions of dollars. It's easy to see how unaddressed vulnerabilities in patient identity security should, if they do not already, represent a major concern for the entire healthcare industry.

Privacy protections regarding online healthcare information initially lacked enforcement mechanisms when first introduced in the early 1990s. However, sweeping changes in regulator standards in the U.S. and worldwide are increasing pressure on healthcare systems to implement digital identity security protocols that provide advanced identity proofing and authentication.

Identity proofing and authentication solutions are necessary to secure patients' data while conveniently providing access to their healthcare information. Navigating the identity security market and choosing vendors can be daunting, especially for organizations prioritizing user experience alongside the secure storage and dissemination of patient information.

This e-book from Daon, a global leader in digital identity proofing and authentication solutions, will explain the challenges, innovations, and benefits surrounding identity proofing and authentication systems and, importantly, how having a strong CIAM (Customer Identity and Access Management) strategy can prepare healthcare organizations for the future of medicine.

Challenges Facing the Healthcare Industry

The pressures mounting in the healthcare industry tend to fall into two main categories: supply/demand and regulatory. These challenges impact an organization's ability to not only stay in business, but to fight medical identity fraud and prioritize UX for their users – the latter two challenges which, thankfully, can be eased by having a CIAM system that is managed by a reliable identity security provider.

Supply and demand pressures

Supply and demand pressures involve the balancing act organizations must perform when it comes to the supply of available healthcare workers and equipment with patient demands in the industry. To keep up with the growing demands on hospitals, clinics, and providers, the supply of healthcare workers will need to increase dramatically, or, their respective workloads will need to decrease dramatically.

Additional supply and demand pressures include:

Cost barriers

While 90% of adults carry health insurance, polling has revealed that more than 40% of adults in the U.S. have postponed healthcare needs due to cost (or had a family member who did). In addition, roughly one-third of uninsured adults are anxious about their ability to afford monthly health insurance premiums, with almost 50% worrying about affording the high costs of meeting their deductible before their health insurance takes over.

By putting off treatments, health issues are likely to worsen, resulting in more significant healthcare problems and higher bills down the line. While efforts have been made to reform the healthcare industry, particularly the added costs of insurance and efforts to increase transparent pricing, experts note that we must make far more progress to prevent expenses from obstructing access to health services.

An aging U.S. population

An aging American population also places an additional strain on healthcare systems due to rising rates of chronic illness as citizens age. For instance, experts predict that cancer cases will increase to 27 million by 2030, up from 17 million cases in 2020.

Aside from cancer, older Americans are also at high risk for experiencing cognitive decline in their later years. According to forecasts from Alzheimer's *Disease International*, there will be 115 million individuals with either Alzheimer's disease or dementia by 2050.

Elderly individuals are also far more likely to experience a severe fall, resulting in potentially life-threatening injuries. Each year more than 300,000 hip fractures result from falls, and the American Hospital Association (AHA) predicts that number will double by 2050.

For these and other reasons, an aging population is forecast to introduce increasing financial pressures within the healthcare system and create more demand on healthcare providers.

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

Rising rates of chronic disease

While older Americans are at the highest risk for chronic illness, people of all age groups are experiencing increasing rates of chronic disease, especially heart disease and diabetes. The number of Americans with diabetes, for example, is expected to rise from 30 million cases (as of today) to more than 46 million by the end of the decade, according to the AHA.

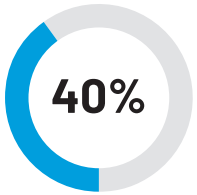
Annual healthcare costs for people with chronic diseases exceed $6,000, five times higher than the yearly healthcare costs of those without diagnosed diseases.

Shortages of healthcare professionals

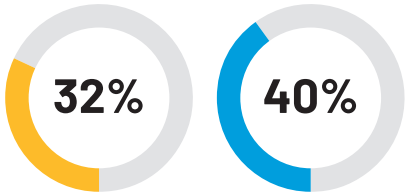
Although the coronavirus pandemic revealed significant shortages of healthcare professionals throughout the healthcare industry, it also exacerbated already existing staffing problems. From 2019 to 2022, the number of doctors who reported feeling burnt out increased from 32% to 40%. For nurses, those rates jumped from 41% to 49%.

These shortages perpetuate high burnout rates that drain talent from the available pool of healthcare workers and can result in avoidable negative health outcomes for patients.

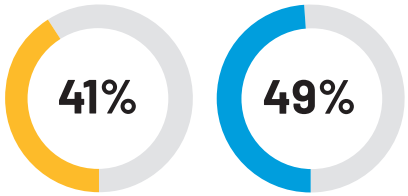
These supply-side pressures are expected to culminate in a vicious cycle for the healthcare industry over the coming decades, with a shortage of roughly 124,000 physicians in the U.S. by 2034, according to the Association of American Medical Colleges.



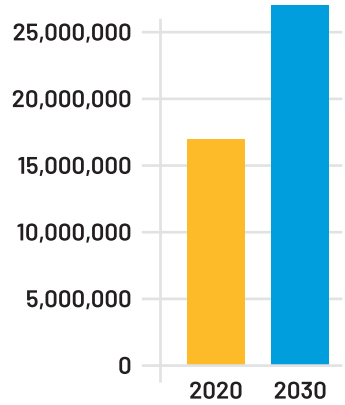
40% of adults have postponed healthcare over cost



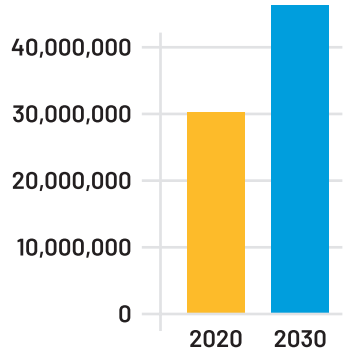
From 2019-2022, the number of doctors who reported feeling burnt out increased from 32% to 40%



From 2019-2022, the number of nurses who reported feeling burnt out increased from 41% to 49%



Cancer increasing from 17 million cases to 27 million cases from 2020-2030



Diabetes increasing from 30 million cases to 46 million cases from 2020-2030

Regulatory Pressures

In addition to these supply and demand pressures, healthcare organizations must also contend with rising regulatory pressures. Over the past decade, privacy laws have grown increasingly stringent, demanding, and enforceable. As we can observe from the trajectory of these privacy laws, we can only expect the rates of regulatory policy enactment to accelerate.

HIPAA (1996)

While identity security, especially electronically, has been an increasingly salient issue for U.S. policymakers, the reality is that European countries have taken the lead on identity protection regulations since the rise of the internet.

In the early 1990s, it became clear that society was undeniably trending towards digital. To begin forming a foundation of data privacy protections, the European Union passed the EU Data Protection Directive in 1995. One year later, the U.S. enacted its Health Insurance Portability and Accountability Act (HIPAA), its interpretation of the European directive. This act was part of a preemptive effort to provide secure sharing of private health information while ensuring that patients had easy access to their health information and medical records.

In spirit, both policies sought a better definition of "personal information" and lay a foundational legal scaffolding to guide the burgeoning growth in digitally shared health information. Although these policies could only anticipate so much at their enactment, the basic idea was that businesses and organizations handling personal information were beholden to maintaining minimum necessary standards of care.

The regulatory environment continued to evolve. By 2002, California enacted data breach notification laws to address perceived shortfalls in federal data security legislation. California's counterparts followed suit until all 50 states had enacted policies.

GDPR (2018)

In 2018, the European Union once again paved the way to improved data security provisions by enacting the General Data Protection Regulation (GDPR), which introduced several additional data protection provisions.

The GDPR also raises the stakes for non-compliance and requires much faster data processing requests than those imposed by existing U.S. standards. While the maximum fine imposed under HIPAA is $1.5 million per year, fines permissible under the GDPR can reach 20 million Euros (the equivalent of $24 million USD) or a staggering 4% of the violator's annual global revenue, whichever is higher.

The GDPR took further steps in identity security by broadening the definition of "personal data" and clarified the three types of personal data relevant to the healthcare industry:

- **Health-related data:** Any data that arises from the delivery of physical and mental healthcare is considered protected personal data.
- **Genetic data:** Due to the sensitive nature of an individual's genetic makeup, which reveals the core of an individual's biochemical identity, all data analysis conducted in labs is protected under the GDPR.
- **Biometric data:** Biometric data is set by an individual's genetic makeup and represents the best method for properly identifying an individual. Anything falling under the umbrella of biometric information, from fingerprints to facial scans, is considered protected personal data that organizations must secure to minimize the risk of identity fraud.

The GDPR also outlines protocols for processing access requests for protected health information: access requests must have the user's explicit consent, be due to a clear and explicit medical need, or due to public interest stemming from public health matters.

The GDPR applies throughout the EU and to any organization that gathers health information on an EU citizen *anywhere* in the world.

Unlike the EU Data Protection Directive of 1995, the GDPR did not prompt a corresponding policy from U.S. federal government. Instead, California again took action with the 2020 California Consumer Privacy Act, which mirrored the added data protection expectations for businesses collecting and sharing personal data. In California, the policy empowered individuals to demand a complete record of information collected on them by certain organizations, and as of 2023, this law applies to both consumers and employees.

Over recent years, these regulations have evolved significantly with the changing cybersecurity environment. Every year, the forms of cybercrime and the technology used by the criminals who perform them continue to diversify and increase in severity and sophistication.

Cybersecurity concerns

Added policy instruments to protect private healthcare information can only be expected to continue snowballing into regulatory cascades and weighing down the burdens on healthcare organizations.

Healthcare organizations have a two-fold cybersecurity conundrum. They are called upon to position themselves to protect patients' financial information and private health data from the real risks of cybercrime while also ensuring that their systems are robust enough to provide excellent customer experiences.

Personal information is currently the most lucrative prize for cybercriminals, especially regarding health data. Data reveals the high value of stolen health records on the dark web, which can sell for as much as 10 times more than stolen credit card information. This presents a risk to patients due to the consequences of leaked private patient information and the possibility that health records could be altered, potentially resulting in severe impacts on patient treatment and health outcomes.

There is also the financial burden of stolen healthcare data. According to data from IBM and the Ponemon Institute Report, the current cost of a healthcare breach is over $400 per stolen record, or roughly three times the cost to resolve stolen records issues in industries outside of healthcare.

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

And, to make matters worse, healthcare breaches continue to increase. According to Verizon's 2020 Data Breach Investigations Report (DBIR), healthcare breaches and incidents rose 71% from 2019 to 2020.

FHIR Protocol

FHIR, or Fast Healthcare Interoperability Resources, outlines standards that exist to define policies for the exchange of healthcare information amongst computer systems. These policies and processes are designed to apply regardless of how data is stored within those systems. By setting these terms, FHIR helps to facilitate the secure sharing of sensitive healthcare information between devices, improving the safety of data sharing and enabling more rapid diagnosis and treatment for patients.

In addition to patient protections and benefits, it also streamlines the information security and HIPAA responsibilities placed on healthcare providers, conserving time and resources.

Tools Needed for the Next Generation of Healthcare Providers

As medicine continues to improve, the importance of software that better manages the complexity of human medical data becomes increasingly mission-critical. Yet, there's no one-size-fits-all option, just like there are no two matching fingerprints. Balancing identity security with functionality and convenience requires carefully selecting the right solutions.

While solutions vary in terms of functionality, understanding the variations in required functionality is easiest to appreciate by considering the differing needs of healthcare organizations by type.

Hospitals

The strategic use of technology is all the more critical given the current challenges facing hospitals. According to the American College of Healthcare Executives, the top issues confronting hospitals today include:

- Workforce challenges
- Financial challenges
- Issues stemming from behavioral health

Hospitals risk making mistakes and failing to properly care for patients without fully staffed healthcare teams. To prevent this, hospitals are employing short- and long-term strategies, including strengthening their workforce pipelines, offering increased staff support, and reorganizing services to efficiently allocate resources. But technology will also need to play a critical role here. The treatment of patients with health problems that vary in degrees of urgency and severity requires providers to have the best tools to remain up to speed on every patient amidst the chaos of most hospital environments. Digital identity solutions will also be necessary for onboarding new patients to reduce workloads through the automation of repetitive functions and integration of healthcare software to minimize instances of human error.

Pharmacies

Even under the best circumstances, manually dispensing medications is time-consuming and repetitive. Patients must wait in long lines for their prescriptions and authenticate their identity using non-biometric (and therefore less secure) methods, like driver's licenses, passports, and security questions ("What's your date of birth?"). As the need for medications increases and the demand for prescription dispensing rises, the number of pharmacies and pharmacy staff will need to increase to meet demand, or we will need secure methods for automatically processing those prescriptions. Per regulations, an automatic dispensing system would need to be free from error and free from the

potential for abuse (like identity or medical fraud), all while still meeting the current performance of in-person medication dispensing. In today's healthcare environment, these dated processes put pharmacies even further behind when it comes to shortages of pharmacy technicians, work-driven burnout, continuing financial challenges stemming from the coronavirus pandemic, and pressures from drug pricing indexes in the face of inflation and medication shortages. Pharmacies must reduce the demands on staff members to prevent burnout and better retain their employees. They will also need improved systems for drug purchasing and inventory management systems, all of which require a more centralized healthcare data information system to manage customer information in real time. The nascent automated dispensing market, which provides the opportunity for decentralized and automatic dispensing of pharmaceuticals, is expected to grow at an AGR of 7.2%, reaching a market size of roughly $8 billion by 2030.

Labs

According to experts, laboratories' top challenges include staffing issues, poor management training, and internal conflict, issues which strike at the heart of efficiency and quality work performance. Like the responsibilities of both hospitals and pharmacies, laboratory technicians must follow straightforward and predictable routines for processing samples and generating lab results. These environments often burst with untested specimens and face tight turnaround times, lest a patient be forced to delay potentially life-saving treatments. Those lab results contain sensitive genetic information, which can only be expected to fall under increasing regulations. Labs and other healthcare organizations can communicate faster with improved identity proofing systems, allowing for more rapid treatments and processing times. Additionally, employees in laboratory settings are often promoted to managerial roles without receiving formal training in developing and applying managerial skills. Because the roles of laboratory technicians and managers differ significantly, software tools to streamline the professional development of lab management are essential.

Independent providers

The Affordable Care Act attempted to streamline healthcare access and reduce overall spending while boosting quality of care and ease of treatment by incentivizing hospital ownership and affiliation with independent healthcare providers. The opposite happened: healthcare spending appeared to increase while health outcomes worsened. With just 49% of physicians working at independent medical practices, patients seeking out independent providers are simply overwhelming the system. For that reason, physicians have been forced to decrease time spent with patients and keep up with increased regulatory requirements for data reporting, all while facing heightened rates of burnout. Independent healthcare providers are less equipped to access the economies of scale enjoyed by their much larger healthcare counterparts. For this reason, technologies that increase efficiency in terms of identity security and authorization can completely underlie

an independent provider's economic advantage. Providers can use identity proofing tools to automate as many repetitive processes as possible to allow time to focus on their patients without feeling rushed or overworked.

Insurance companies

Due to the complex nature of the economics of health insurance, consumers often feel barred from what they often perceive as overly opaque and arbitrary systems. Common challenges facing healthcare insurance companies include:

- The need to develop improved ways of measuring consumer insights
- Offering better customer experiences
- Improving access and coordinated leveraging of available internal and external health data
- Adopting improved facilitation mechanisms to promote clear communication with customers

More than anything, insurance providers must become more accountable, which will require systems that minimize the complexity of internal structures and allow for more centralized management of data storage and sharing. Although insurance companies are not healthcare providers, they are still held to the same patient access standards about private healthcare information. These companies must have identity security and authorization tools capable of quickly and securely processing information requests.

These various healthcare organizations will also need tools to streamline reporting and demonstrate compliance with regulators. By streamlining these monitoring and recordkeeping processes (all of which will involve secure record-keeping of personal health information and patient-provider interactions), centralized oversight tools will help organizations to maintain compliance.

Utilizing Identity Proofing Solutions in Healthcare Organizations

Throughout these types of organizations, identity proofing can improve the patient/consumer-provider relationship by ensuring that communication channels remain secure. One of the most transformative technologies to accomplish this are identity and access management (IAM) systems.

These systems revolutionized relationships by facilitating interactions at the intersection of data, economy, and society. IAM systems were designed primarily for the secure sharing of information within organizations and involved the creation of barriers to keep sensitive information from being shared with unauthorized users outside of the organization.

As digital systems evolved, so did the need for architectures capable of optimizing interactions between brands and their customers, which gave rise to customer identity and access management (CIAM) systems. Customer identities far outnumber employee identities when it comes to scale. In fact, customer identities can scale up to the hundreds of millions, so organizations in the healthcare industry are being exposed to the potential for vulnerabilities and accidents at a tremendous scale.

CIAM systems can promote innovation by supporting growth with no-code/low-code development capabilities, which allow for systems built more directly from the needs of healthcare organizations.

In addition, consumers increasingly expect integrated applications for online identity proofing through linking social media and other online consumer accounts (Microsoft account, LinkedIn, etc). To meet the demand for convenient access to patient medical information, healthcare systems must adopt identity security and authorization mechanisms capable of offering those conveniences at scale.

Healthcare patients also expect to have a single, integrated account with their provider, despite the various points of contact and interaction that exist within that single healthcare provider. So, not only must the organization keep information both secure and highly accessible, but the tools employed must also be highly centralized to streamline information sharing.

User onboarding and authentication are critical because they represent the initiation of interactions between patients and the digital applications provided by their healthcare providers. As the Smart Card Alliance explains: "While dependably accurate identification and authentication seems like something that should already exist in healthcare, it does not." This poses an existential threat to the healthcare system as a whole.

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

The recent *Medical Identity Theft Report*, sponsored by the U.S. Department of Health and Human Services, reveals that several avoidable oversights introduce inaccuracies to the identity proofing process. Some of these oversights include:

- Incomplete patient registrations
- Redundant data entries and names
- Misspellings

With so little emphasis on authenticating identities in the healthcare industry, these largely unaddressed problems contribute to an environment with rampant medical identity theft.

Utilizing identity proofing and authentication solutions allows healthcare providers to:

Better protect patient health records

Healthcare organizations without sophisticated systems to verify patient identity can be defrauded when an unauthenticated person accesses a verified patient's health services or data. In 2019 alone, 41 million patient records were breached. The increasing frequency of these healthcare breaches has resulted in as much as 39% of patients reporting a concern that hackers would steal their sensitive health information. Identity proofing and authentication solutions can ensure on-time payments, correct medical records, and minimize the risk of medical fraud. With elderly individuals specifically, patients can sometimes supply incorrect personal information to healthcare providers, either on purpose (if they are a fraudster in disguise) or by accident.

Remove accessibility barriers for online access

Unaddressed barriers can severely limit patient access to healthcare providers and private health information worldwide. One survey found that common frustrations limiting consumer access included cumbersome log-in procedures, reluctance to enter private information, and difficulties creating passwords with more involved requirements. Healthcare professionals can access patient information remotely and securely in real-time by helping to verify and authenticate patient identities through passwordless factors. By combining the power of biometric authentication with software designed to manage authentication processes at the macro and micro levels, patients enjoy more reliable and convenient access to their healthcare providers.

Authenticate patient identities remotely

Remote identity proofing and authentication is the most significant challenge when designing and building resilient identity proofing systems for healthcare providers. Still, experts foresee dramatic increases in remote healthcare services due to rapidly advancing biometric technologies. The global telehealth market is expected to grow at a compound annual growth rate of 24% between 2023 and 2030, driven primarily by a rise in telehealth service offerings and supported by significant innovation in telehealth software.

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

Improve healthcare equity

The U.S. Department of Health and Human Services (HHS) lists telehealth as a burgeoning form of healthcare equity, allowing access to life-affirming care for underserved communities. Changes and improvements to the way that people access telehealth can move the needle even closer to allowing a health gateway for rural, older, and low-income patients, or even those who are differently abled, immigrants, or who have limited digital literacy. Among the access recommendations from HHS, "technology designed with equity in mind when it comes to speech recognition and health prediction algorithms." Improved identity proofing and secure access technology fulfills this objective and makes telehealth more practical and equitable for all patients.

Simplify processes

Identity proofing and authentication systems will centralize patient health information, making it easier to catch errors. Identity proofing and authentication, which occur at the beginning of a customer-brand interaction, help streamline and improve patient intake processes while serving as a first line of defense against attempted medical fraud.

Allow physicians to write prescriptions online - securely

Without optimized processes for prescription writing and medication pickup, patients may be unable to continue taking their medications, negatively affecting patient health outcomes. Data from 2009 to 2018 demonstrate an increase in web-based prescription-filing behavior among U.S. adults.

Onboard remote healthcare employees

Facing such significant shortages in healthcare staffing and a current professional environment heavily favoring remote work, learning new software systems remotely can place a perpetual drain on IT teams, professionals, and other workers within healthcare organizations. By integrating onboarding into the architecture of identity proofing and authentication technologies, these systems can help to streamline hiring processes while ensuring that all members of an organization have the training they need to best serve their respective roles.

Onboard users

In addition to the onboarding and authentication benefits for organizational members, these same processes also have a tremendous impact on patient identity journeys in several respects, including:

- An overall enhanced patient experience
- Improved outcomes for data security
- Increased administrative efficiency
- Scalability and agility of systems that allow for more rapid achievement of compliance as policymakers enact new identity security regulations

Benefits of Identity and Access Management (IAM)

By emphasizing identity and access management (IAM) in the design of healthcare CIAM system architecture, healthcare organizations can integrate identity security into customer experience applications without causing those systems to suffer from a UX perspective. There are seven key benefits that IAM security imperatives bring to the CIAM systems designed for healthcare organizations:

Internal workflow optimization

With built-in reporting (with more sophisticated systems) and out-of-the-box multi-factor authentication (MFA), workflows are simultaneously secured and streamlined, giving users and organizations choices when it comes to how they authenticate themselves, and data to provide insights into how the process is working for any user.

Compliance and security

The improved optimization of internal workflows contributes directly to maintaining compliance and security. Optimization is made possible by simplified and transparent authentication protocols, which are much easier to monitor and update.

System integration

By bringing all areas of patient health information access into one platform, healthcare organizations achieve a centralized view of their patients, allowing them to make faster and more informed decisions.

Cost reduction and efficiency

The boosted efficiency, achieved through the automation of identity security and authentication processes, allows healthcare organizations to price their services and treatments more competitively.

Easier patient journeys

By adopting more agile and well-adapted systems, healthcare organizations pass financial benefits onto their patients, allowing for more convenient and transparent patient journeys.

Improved patient care outcomes

Ultimately, by facilitating patient care through an identity proofing and authentication platform, the patient-provider relationship can reach new heights due to increased levels of trust and mutual understanding. With a greater sense of clarity, patients are better able to access the medical care they need, and healthcare providers are more capable of delivering it. The result is an improvement in patient care outcomes.

Meeting the Healthcare Needs of Tomorrow

Identity Proofing and Authentication Solutions for Healthcare Organizations

Your Identity Proofing & Authentication Partner of Choice

Daon, the well-established Digital Identity Trust company and industry leader in identity proofing and authentication solutions, is expanding its reach as a partner to organizations throughout the healthcare sector. By channeling the expertise of its veteran IAM development strategists, Daon is now an essential presence in healthcare's ongoing fight against cyberattacks, medical fraud, and dated systems that no longer best serve the needs of patients or providers.

Our philosophy is to push the limits of innovation with respect to information security in a society where so many of our identities exist in a digital environment. We're a proven leader in optimizing relationships between organizations and their customers, and we're charging forward into an industry wrought with uncertainties and vulnerabilities, ready to elevate patient care to a level not yet experienced anywhere in the world.

We recognize that the sophistication required to develop resilient and ideally suited CIAM systems requires a collaborative effort from various skilled professionals. Daon's capabilities, technology, and experience are unmatched when it comes to identity proofing for healthcare organizations.

Daon's available solutions and technologies have secured over one billion identities and execute over 250 million daily authentications. With over 20 years of experience, we know we're the best in the business and are ready to put that expertise to work for you. Visit our website to learn more and schedule a consultation today!

www.daon.com/healthcare

Daon®

The
Digital Identity Trust
Company