WHITEPAPER

Envisioning the future of digital identity in healthcare

THROUGH THE POWER OF DIGITAL IDENTITY, HERE IS WHERE HEALTHCARE IS HEADED IN THE NEXT DECADE

Kristina Cairns
Director, Product Marketing

Jeremiah Mason
Manager of Research & Discovery

Wes Wright
Chief Technology Officer

imprivata®

Digital identity has become ubiquitous in today's society. Whether you're accessing your phone with face recognition, logging in to your banking app using your fingerprint, or using the classic combination of email address and password to open your work laptop, chances are you're invoking digital identity dozens of times every day. Identity and access management (IAM) originated as a set of technologies primarily used in industries where highly sensitive data was stored in isolated backend systems. As more and more aspects of daily life become digitized, however, digital identity has become the control plane for human-to-device and human-to-organization interactions of all kinds – from social media and banking, to retail, education, and healthcare.

Ironically enough, this technology that was devised to secure systems and data, and ensure personal privacy, is now, in some situations, increasing risk precisely because it has become so prevalent. The sheer number of digital identities associated with individuals today multiplies the points of vulnerability where identity theft, financial damage, and data loss can occur. There is no starker example of this than the wave of ransomware attacks that began targeting hospitals and healthcare service providers in the United States in the fall of 2020.[1]

Hospitals and healthcare facilities: Uniquely vulnerable

In late October 2020, the U.S. Department of Health and Human Services, the FBI, and the Cybersecurity and Infrastructure Security Agency issued a joint cybersecurity advisory warning healthcare organizations of an "increased and imminent cybercrime threat." Shortly thereafter, multiple hospitals and healthcare facilities in Oregon, California, New York, and other states experienced ransomware attacks. The common attack vector with these incidents? Compromised digital identities, most often stolen through phishing emails. Once an attacker captures the identity of a hospital employee, they can use those stolen credentials to move laterally across the organization's network and gain access to sensitive systems and data. The ultimate target? Usually the electronic health record (EHR) system, which, when taken offline, effectively paralyzes essential hospital functions.

1 https://searchhealthit.techtarget.com/news/252491502/Cybersecurity-advisory-a-call-to-arms-for-healthcare-CIOs
https://www.reuters.com/article/us-usa-healthcare-cyber/building-wave-of-ransomware-attacks-strike-u-s-hospitals-idUSKBN27D35U

These incidents clearly show why the digital identity challenges for the healthcare sector are unique. Hospitals are charged with securing protected health information (PHI) as a regulatory imperative, yet they are also, in most cases, large sprawling organizations employing hundreds or thousands of medical professionals, clinicians, administrators, and staff. This distinct organizational model calls for a fine-grained hierarchy of access rights to various systems and data. Consider also that the ways in which data flows through hospitals and healthcare organizations is unique as well. A patient scheduled for a surgical procedure could have their medical record data travel through dozens of touch points, from admissions and imaging to the surgery department, pharmacy, billing, and more. It's not a surprise then, that healthcare IT decision makers are increasingly realizing that their digital identity needs are not readily addressed by off-the-shelf IAM products, and that solutions optimized specifically for healthcare applications are essential.

Five principles for digital identity in healthcare going forward

The context for the future of digital identity in the healthcare sector is clear:

- Hospitals and healthcare organizations – and by extension, clinicians, IT staff, and patients – are at higher risk for cyberattacks than most other industries. Security publications that track cyberthreats regularly place healthcare at or near the top of their lists of targeted industries.
- Organizational make-up, and unique IT systems and architectures, compound the sector's already complex challenges posed by the need to collect, store, and share PHI.
- Digital identity is an indispensable tool for privacy and security, but continued high rates of ransomware attacks, data breaches, and credential compromise clearly show that generic IAM solutions – which in most cases were originally designed for financial services, government, or retail applications – can be a serious point of vulnerability in healthcare settings.

Given this context, the question now is how to harness the power of digital identity to make life better for everyone involved in the healthcare industry 5 or 10 years from now. We believe that, going forward, digital identity for healthcare needs to be based on five principles:

1. SINGLE HOLISTIC IDENTITY SOLUTION

As hospitals added new technologies over the years, it was usually in the context of departmental clinical systems: radiology installed a new mammography system, pathology got new centrifuges, medical records expanded on its EHR, and so forth. With increasing regulatory mandates to secure PHI – now easily shareable as digital data produced by these systems – hospitals needed ways to secure each of their departmental clinical systems. And in the early days of the digital revolution, each would have had its own credentialing and secure access processes. That legacy has left most hospitals with very complex identity strategy structures where the organization will often have one tool for provisioning and de-provisioning, another for multifactor authentication, another for single sign-on, and a fourth for fast smartcard-enabled access.

Today, IT security staff find themselves having to stitch and weave together all of these products to try to create a coherent user experience for clinicians and staff. But with multiple loosely integrated identity products and multiple upgrade schedules and patches, the potential for problems that can lead to vulnerabilities is high. In an ideal world, a hospital would rely on a single holistic solution for managing digital identities that provides full security for data and systems, privacy for patients, and easy yet tightly controlled access and authorization for users. However, this is not always easily realized or feasible.

What we should be working towards is a decentralized identity infrastructure that will allow the various different systems within an organization to accurately map back to a single identity held by the user. This will give hospitals the power to instantly and automatically provision, de-provision, modify access rights, and accurately report on all their users across the digital continuum. Disparate systems will now be able to talk the same language and exchange data to ensure they are always talking to the correct entity. The dream of one heartbeat, one identity will become a reality and federation across organizations will be easier and faster than ever.

With increasing regulatory mandates to secure PHI – now easily shareable as digital data produced by these systems – hospitals needed ways to secure each of their departmental clinical systems.

2. IDENTITY ASSURANCE

Digital identity is only as strong as the data it's built upon. Individual identities, whether for systems, devices, or users, must be a cumulative collection of attributes that can set a foundation of assurance that strengthens over time. These attributes can start with data points such as demographics, professional credentials, known trusted devices and locations, etc. But ultimately, we should be looking at the identity assurance imperative as a tripod:

1. Identity governance
2. Identity proofing
3. Identity assertion

First, identity governance sets up the right access for the right user. Then, you need to know who that user is and be very sure of it through a formal identity verification process. From there, users are bound to strong authenticators that allow them to assert their identity, granting access to systems to which they are authorized. All three processes – which are approached as separate endeavors in most healthcare settings today – will be united and automated in the healthcare digital identity solution of the future.

3. ACCESS AND AUTHENTICATION STANDARDS

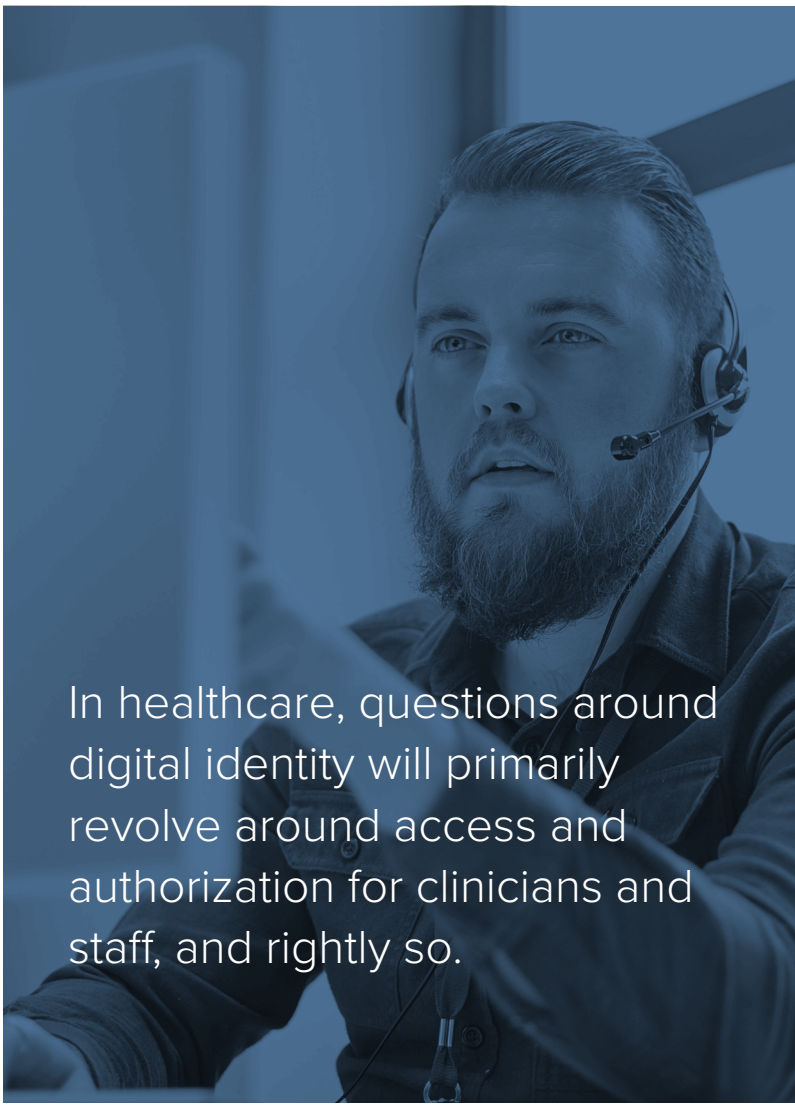
For decades, public key infrastructure (PKI) has been a core element in digital identity systems as the method for securing federated identities. Yet PKI has so many moving parts, such as certificates, registration authorities, directories, and policies, that it's very cumbersome to manage, and becomes progressively more so as a user base grows over time. Happily, new standards for securing federated identities have emerged that will enable the identity systems of the future to take increasing advantage of biometrics and passwordless authentication.

- **Security Assertion Markup Language** | Universally known as SAML, this standard enables single sign-on through the exchange of authentication and authorization data. In a hospital setting, it would enable an administrator who's logged into the organization's intranet to then access any number of other systems – EHR, billing, Workday, Salesforce, etc. – without having to provide credentials a second time.
- **OpenID Connect** | This standard will be familiar to anyone who's used their Google account to sign in to a retail website; essentially a form of passwordless access. In the healthcare setting, the benefits of this technology are multifaceted. It eliminates the drawbacks of sloppy password practices (which has huge implications on the ransomware wave) and promotes better security and ease of use for care providers who can now access clinical systems and devices through biometric identification.

- **Verifiable Credentials** | Blockchain has taken some heat as a buzzword, but it's the underlying technology for a W3C standard known as Verifiable Credentials, which has much promise in the healthcare setting. The idea is to have a verifiable identity or verifiable elements of an identity that are distributed in a widely available system of record – a system where any party can verify certain claims about an individual.
- **Fast IDentity Online (FIDO)** | The FIDO Alliance is an industry consortium committed to developing and promoting authentication standards that reduce reliance on passwords. FIDO does use PKI, but in a manner that is invisible to the user. Once a device is registered, the client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user–friendly and secure action such as swiping a finger or entering a PIN. If used, biometric information, much like the PIN, never leaves the user's device, which increases privacy and security.

4. PORTABILITY

Looking at all the emerging standards listed above, it's clear that the identity industry is determined to address issues around ease of use and make progress toward a passwordless future. The larger underlying problem, however, is portability. Why do people reuse passwords over and over again? Because they have so many different digital identities! In healthcare, questions around digital identity will primarily revolve around access and authorization for clinicians and staff, and rightly so. Consider, for instance, a doctor who works at more than one hospital. Ideally their identity would be federated so that when they need to see patients at facilities other than their primary location, they would have access to the systems and areas of the hospital necessary for carrying out their duties – even if their ID hasn't been fully onboarded for that particular location. This use case is something that is being tested on a pilot basis within the UK's NHS, but is not yet common in the U.S.



Consider also how digital identity could come into play to improve the experience, and perhaps even outcomes, for patients. Many organizations in industries like retail and banking regard identity as a key enabling technology with know-your-customer (KYC) efforts and other kinds of personalization in customer-facing interactions. How would this work in healthcare settings? Industry observers believe this would require either a centralized national identity or an identifier based on the verifiable credential concept, which would be based on the distributed ledger approach. In either case, portability paired with strong authenticators enables the patient to gain entry to a front door, but then having that front door open in turn opens up many other doors within the hospital or healthcare setting.

5. PRIVACY

We discussed above the issue of having so many different system silos where identity is the one thing that's weaving the underlying clinical systems and data together. The problem is that the security behind this type of architecture is lackluster. The question has been: what was the process to create that identity? How can you be sure, and can everyone within the organization rely on that initial process? In many cases the answer to these questions was: we're not sure. And that can be a problem, because controlling the access to core EHR and other systems is key to protecting patient privacy and assets. Digital identity is a key part of knowing who is accessing what data, where, and when. Without proper knowledge of all identities, their access rights, and what they are doing, patients and even staff do not have privacy.

This is where data will become more critical than ever. Hospitals will leverage the power of AI and ML to accurately report on access rights, who is accessing what and where, violations, and missteps in process. With powerful insights, abuse of privacy and access will not go unnoticed, and remediation will be swift and automated.

Going forward, and as the internet of medical things (IoMT) begins to mature, the question will become: who's on your network? Should this person/device/application be accessing those resources, and can you provision that digital identity down to a granular enough level? If so, then you can say, this is a nurse named John. He can have access to patient data for these patients alone. The patients that are in somebody else's section, on a different floor? John shouldn't have access to that patient data. That's where digital identity is going and must go in the future. Laws like GDPR and the California Consumer Privacy Act have elevated privacy of the individual to such an extent that it needs to be the central organizing principle for any system of digital identity, especially in healthcare.

With powerful insights, abuse of privacy and access will not go unnoticed, and remediation will be swift and automated.

The road ahead

It's hard to overstate that the digital identity challenges facing the healthcare sector are complex and multifaceted. As an industry under assault by cyber attackers, the first priority for healthcare IT executives is to protect and secure the systems, data, users, and patients in place right now. At the same time, the imperatives for establishing a more effective and beneficial digital identity paradigm are quite clear. A holistic solution for managing and governing the digital identities of all clinical staff, medical record systems, devices, and applications within the healthcare organization. A capability to manage identity governance, identity proofing, and authentication assurance as a unified process. Simple, passwordless but strictly regulated access and authentication for users. And always and everywhere, privacy for the individual and their data. Taken together, all of this will lead us to toward a better life for IT, clinicians, and patients.

Imprivata is the digital identity company for healthcare. Please visit our what we do page to learn about how our digital identity strategy helps healthcare delivery organizations manage identities across complex ecosystems.

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com.

DI-WP-envisioning-future-0121