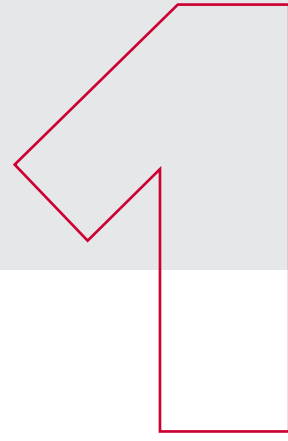




The Digital Identity Report

Solving healthcare IAM challenges



Introduction

In recent years, the healthcare industry has been hit hard with pressure from payers, increased regulation, a higher level of competition, and a global pandemic, unprecedented to the modern-day system. Throughout these challenges, digital transformation has been accelerated, and a digital identity strategy has become imperative.

As a massive, multi-level industry, healthcare continues to run into unique obstacles during its digital transformation due to a long list of complexities, including staffers with multiple roles and access, patient data security, frequent cyberattacks, and a steady stream of federal regulations and other mandates.

The solutions to security and workflow issues that have succeeded in other fields are not synergistic with the many factors that healthcare faces. A new digital identity strategy is needed; one that tailors current identity and access management practices to address the specific challenges that healthcare faces every day.





“ Healthcare professionals, faced with securing an increasingly complex workflow automation environment, can’t wait. The security landscape will only become more diverse and complex over time. It is important to select a vendor that can deliver a single identity and access governance solution that is capable of scaling as organizational needs change.

”

FROST AND SULLIVAN¹

¹“Delivering Frictionless Security to the Clinical Workflow: Access and Identity Management the Key to Workflow Efficiency,” Frost and Sullivan White Paper, Mike Jude, Ph.D.



2

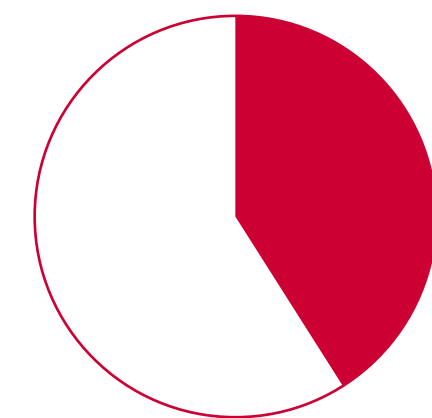
Identity and access management

In an age in which immediacy is expected, medical professionals need secure access in more places at more times, with higher expectations for engagement and patient satisfaction.

But top-level security breaches have proven that there are vulnerabilities in the current system, whether on-premises or in the cloud. In fact, 41% of all security breaches in 2019 occurred in the healthcare industry.²

The adoption of cloud services and mobile devices by healthcare organizations has allowed for more immediate access and interaction. However, these new assets have come with increased security regulations, and protection always comes at a cost. In the case of healthcare, that cost can be incurred through patient care.

This is where identity and access management (IAM) of trusted digital identities comes into play.



41%

The healthcare industry accounted for 41 percent of all security breaches in 2019

² "Beazley Breach Briefing – 2019," Beazley

Executed effectively, IAM can mitigate risk, diminish fraud, and strengthen overall objectives through:

- **Identity governance**

Role-based provisioning, compliance reporting, risk dashboard, de-provisioning, ID proofing and record keeping for electronic prescribing of controlled substances (EPCS)

- **Shared mobile device lifecycle and user management**

Automated device provisioning for clinical and patient-facing devices, cloud-managed device imaging, seamless device access management, SSO into mobile applications, , asset management, secure data sanitization

- **Single sign-on and clinical access**

Enterprise single sign-on (SSO), virtual desktop access, shared clinical workstations, web SSO, mobile and medical device access, walk-away security, self-service password reset

- **Multifactor authentication**

EPCS, remote access gateways, adaptive authentication, hands free authentication, phone-based authentication, biometrics, cloud applications, clinical workflows

- **Patient identification**

One-to-one matching with medical records, patient- and registrar-friendly user experience, dashboards to monitor and encourage adoption

- **Secure communications**

Secure, HIPAA compliant communication across mobile devices and desktops, organization-wide groups, broadcast messaging

“IAM encompasses tools and best practices to manage identities and access across an enterprise’s workforce and customers, to manage risk, reduce fraud and other losses, and enable business imperatives.”

GARTNER³

³ “Identity and Access Management Primer for 2019,” Gartner PDF



A truly successful IAM implementation should add security and compliance without time-consuming inefficiencies, while also streamlining and facilitating for IT staff the management of the people, devices, and applications in their healthcare delivery organizations (HDOs). Without these built-in efficiencies, technology interaction can contribute to clinical burnout for physicians, and IT staff can be stuck in a continuous reactive cycle of constant manual management instead of being strategically focused on supporting the organization. In the context of healthcare, this could be referred to as a “digital identity crisis.”

The digital identities of people, devices, and applications allow all of these entities to interact, exchange, and store information between them. But the volume of these interactions and the need to secure them all has created complexity; this often leads to workarounds, thereby opening the door to more potential cyber risks. In response, healthcare companies have sought IAM solutions to manage that complexity.

“ The interaction between clinical staff and technology in a hospital’s core business process is unusually — perhaps even uniquely — complex. It has been estimated that a physician or nurse in a single shift may deal with 18 patient cases, requiring use of various specialized electronic medical devices and access to patient records via as many as 14 different software applications from terminals in different locations within the care facility or off-site. ”

KUPPINGERCOLE⁴

⁴ “Healthcare IAM: Enhance the Clinical Workflow,” KuppingerCole





A hospital staff is made up of a litany of different jobs and different roles — someone who is a nurse every morning may also be a department head every afternoon. This requires one person to have multiple levels of access at different times of day, which is only one example of the many complications in healthcare. Users range from nurses to surgeons to physician assistants to doctors and beyond — not to mention vendors, affiliates, locums, contractors, and IT departments. There are a multitude of moving parts to the industry that require consideration when adopting new technology.

The environments in which these individuals operate are distinctly complex and varied as well. For instance, the shared workstations and mobile devices used by clinicians on the frontlines of healthcare require one set of IAM solutions, but providers may use an array of devices and applications in multiple locations that require another. In addition, the systems being used can be a mix of legacy applications and cloud-based infrastructure. These complications increase exponentially in the vast expanse of various healthcare roles.

Because of the importance of healthcare data, federal regulations and other mandates govern best practices and, often, rules that must be followed, creating more boxes for systems to check. And because healthcare is aggressively targeted with cyberattacks, protecting patient data at all times continues to be paramount.

In a perfect world, IAM would address the digital issues facing healthcare by tightening security on every workstation and device, whether on-premises or cloud-based, awarding appropriate access to each user, and following all mandates. But healthcare has proven too complex an environment for traditional, cross-industry IAM practices and requires more specialized, comprehensive IAM solutions, purpose-built for the healthcare industry and its unique needs.



3

Healthcare's digital identity crisis

While other industries have embraced IAM solutions either built for them or effective for cross-industry purposes, healthcare stands apart due to:

- The variety of roles within it that require particular access
- Users sharing devices and workstations
- The need to house confidential data that is very frequently under attack
- The continuous growth in complexity in relation to devices, users, applications and locations
- Operating in an environment that is highly regulated, where demands are immediate and can easily become chaotic

IT teams must provision the digital identities of users with the exact specifications they need to get the correct level of access their multiple roles require for both cloud-based and on-premises applications. Performing this task manually is error-prone and labor-intensive, signaling the need for a system that can correctly and efficiently provision users through automation.⁵

Simple access has become anything but simple. Devices such as thin and zero client technology, as well as tablets, mobile phones, patient monitoring devices, medicine dispensing, and refrigeration devices, have complicated things significantly — not to mention names and passwords, security measures for anywhere and anytime access, and the challenge of many users operating shared, enterprise-owned devices.

With more mobile and thin-client devices being used, IT departments need to deploy and secure an increased number of access points. HIPAA and HITECH guidelines sap these resources of efficiency in the name of security, and SSO is not always shared with the growing collection of devices among clinical and non-clinical users.⁶



⁵ "The Unique Considerations for IAM in Healthcare," Gus Malezis, President and Chief Executive Officer of Imprivata ⁶ Ibid

Cyberattacks have been finely tuned to break through common usage of weak passwords, accessing credentials and sensitive data and making headlines the world over. A transparent security response is needed to protect data without slowing down efficiency. Multifactor authentication can accomplish this — but only if it is consistent across all workflows, which is not always the case.⁷

Time is always of the essence — even more so in healthcare than other industries. And as we learned with the COVID-19 outbreak, readiness for the unexpected is critical. Generic digital identity systems that don't align with healthcare's specific needs aren't an option. Piecing one together from multiple providers is also not ideal, as it will result in a disparate system.

Healthcare professionals are much better off with a single vendor who addresses the majority of their problems. Otherwise, the issues that can arise may lead to financial hits, performance drop-offs, and clinician and patient record management issues, all of which can have grave consequences. In the worst cases, they can jeopardize the safety and lives of patients.



⁷ “The Unique Considerations for IAM in Healthcare,” Gus Malezis, President and Chief Executive Officer of Imprivata



Experts at Johns Hopkins have calculated that more than 250,000 deaths per year are due to medical error in the United States⁸ — almost 60 percent of which were attributable to incorrectly identifying the patient.⁹ This can happen because of spelling errors, phonetic typos, numeric transpositions, language barriers, fraud, and/or incomplete or duplicate records; but no matter *why* they happen, they can result in disaster for the patients, hospital, and provider.

Correcting patient database records can be a significant expense; for large hospitals, this can add up to millions of dollars per cleanup every few years.¹⁰ But the biggest problem with this response is that it is exactly that; a response, and not a preventative measure.

Healthcare needs a process that covers the whole scope of the industry, providing an efficient user experience for workers and providers on the move while keeping the vast amounts of data they work with secure. It must satisfy regulatory compliance and audit requirements — specifically for healthcare. And it must function in a way that eliminates problems, rather than simply reacting to them.

Annual deaths caused by medical errors in the US:



~60% caused by incorrectly identifying the patient.

⁸ “Experts at Johns Hopkins have calculated that more than 250,000 deaths per year are due to medical error in the United States,” Marty Makary, M.D., M.P.H., Study Questions Quality of U.S. Health Data, April 2015

⁹ “Medical Error” Carver N, Gupta V, Hipskind JE. February 16, 2020

¹⁰ “Using Health Informatics to Tackle Duplicate Medical Record Issues,” American Health Information Management Association, Shannon Harris, MBA, RHIA, and Shannon H. Houser, PhD, MPH, RHIA, FAHIMA

At the root of these concerns is the lack of consistent and uniform identity management, with a solid set of policies, procedures, and technologies. To be effective, the global healthcare industry must adopt modern technologies to protect its patients, providers, and healthcare delivery organizations.

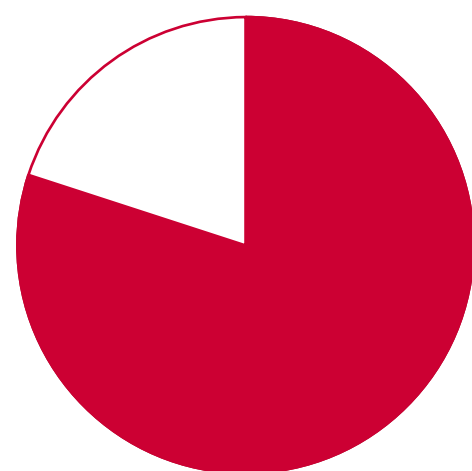
The right platform should enable healthcare providers to do their jobs and focus on patients; to seamlessly coexist with technology that helps them deliver care while maintaining the highest security. It should be affordable to purchase, install, deploy, and use, and be available from a single, trusted vendor for the benefit of integration and long-term strategic partnership.



4

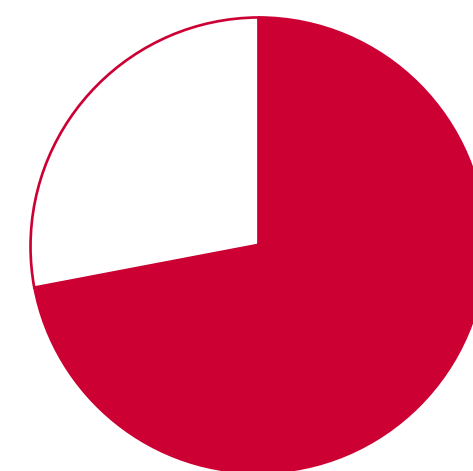
Passwords, passwords, passwords...

Passwords are a problem, and it's easy to see why:



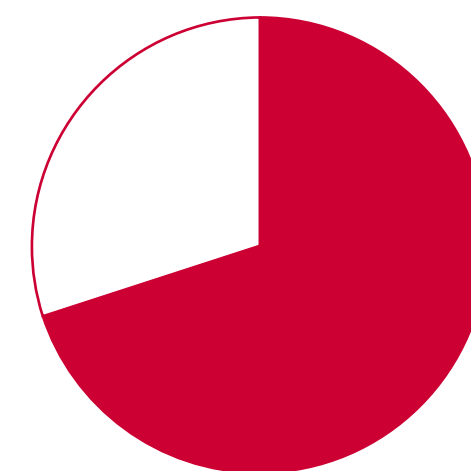
80%

of breaches involve weak
or stolen credentials.



72%

of people have trouble
remembering passwords.



>70%

of employees reuse
passwords at work.



Passwords are the main target of cyber criminals, because a username and password unlock access to corporate systems, data, and intellectual property. In order to keep patient data safe, hospital workstations are always locking, and users are constantly entering and reentering their credentials.

In an industry where every second counts, there is a need for one seamless platform to streamline this process.

“ Contrary to the popular saying that “security is everybody’s business,” the physicians and nurses in a hospital believe that their business is saving lives. ”

KUPPINGERCOLE¹¹

¹¹ “Healthcare IAM: Enhance the Clinical Workflow” KuppingerCole, 2019

5

The right platform

The challenge for healthcare has arisen in part because IAM has traditionally been solved in piece parts. While there have been solutions developed for general obstacles to digital transformation, there remains a need for efficient, economic, comprehensive IAM solutions developed specifically for the healthcare industry, by a company that understands healthcare.¹²

**“Under many current systems
“...a clinician may have to authenticate
to some system or other 70 times in
a single work shift, using different ID/
password combinations.”**

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE¹³

”

While remaining compliant with HIPAA and all other relevant regulations, those solutions must include:

- Automated provisioning and de-provisioning
- Precise role-based access controls
- Streamlined auditing processes and analytics
- Attestation and access certification
- Seamless badge-tap access to all endpoints
- Anytime, anywhere access to on-premises, mobile, and cloud applications

User access should be provisioned and updated as needed. Automating this process comes with the significant benefits of avoiding manual errors and reducing infrastructure cost. With the ability to execute identity policy across all users, devices, and both cloud and on-premises applications, patient and hospital data can stay secure.

¹² Beazley Breach Briefing – 2019, March 21, 2019

¹³ “Report on Improving Health Care Industry Cybersecurity”. Health Care Industry Cybersecurity Task Force, June 2017, p.32

With components like multifactor authentication and single sign-on, users should be able to enter one complex password and tap a physical badge used in concert with proximity-based readers. For the rest of the shift, their identity would be verified; all a clinician would have to do is tap their badge to access the system.

This would cut down on the vulnerabilities of a system in which users are logging in all the time, providing opportunities for cyberattacks. In addition, the system should provide identity governance and compliance, integrate with clinical workflows, and limit security gaps.

The proper system should feature cutting-edge innovations produced by the industry in recent years, such as walk-away security solutions for shared workstations using BLE technology, hybrid cloud platforms for SSO, Bluetooth-enabled mobile phones to streamline clinical workflows, and mobile management solutions focused on shared devices. Ideally, it should be able to integrate with core strategic investments of healthcare organizations to ensure ROI not only of its own solutions, but other technology as well, maintaining relationships and deep integrations with key clinical applications, like Microsoft, VMware, Epic, Cerner, and Meditech. Over time, these partnerships can be expanded in the areas of clinical access, patient identification, virtualization, desktop delivery, clinical mobility, communication, and medical devices.



By cutting out tedious practices like shadow IT policing and constant password resets, productivity can go up and allow an enterprise to grow: independent studies have found that, “On average, a single sign-on product saves around 45 minutes per clinician per shift.”¹⁴ If 100 clinicians save about 45 minutes a shift, five shifts a week and 20 shifts a month, that’s a total of about 1,500 hours saved per month.

Taking into account the many trouble spots in healthcare’s digital transformation, the right platform for the industry would provide precise access for individual users while maintaining ironclad security of patient data. These elements should be strengthened as needed so that ROI can grow across the board and problems can be erased before they can occur. Most crucially, this platform would come from a company that has its finger on the pulse of healthcare.

Healthcare always has to be ready for whatever is next, from cyberattacks to pandemics. Managing trusted digital identities before events like these occur, and not just in response to them, allows us to be ready for what may come in times of crisis, now and in the future.



¹⁴ “Mahaska Health partnership saves clinicians 45 min/day with fast access to EMR applications,” Imprivata.com

6

A trusted vendor, partner, and solution

The world is only growing more complex. Digital identities have eased the exchange of critical information, but healthcare's massive volume of users with varying roles has led to complexities and security risks, and current IAM solutions do not address *all* of healthcare's needs. Digitization should allow this crucial industry to operate both securely *and* efficiently, and Imprivata has the solutions to help it do so.

With 500,000 hours of clinical, workflow, and IT experience implementing solutions in HDOs, we have gained the trust of over 2,200 healthcare customers and over eight million providers using our products. Imprivata has developed answers to critical network questions that have moved the healthcare industry forward. We are the single-vendor solution that securely integrates with clinical workflows.



“

Our history, market presence, and understanding of clinical workflows enables us to continue to solve the challenges healthcare organizations face today, as well as the challenges healthcare organizations will face in the future.

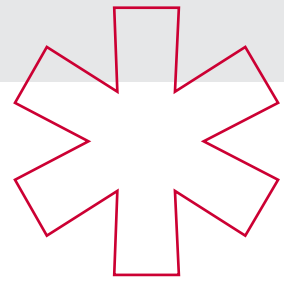
”

IMPRIVATA.COM



We are uniquely positioned to enable healthcare securely, not just because of our solutions and partner ecosystem, but because of our global clinical experience and our understanding of healthcare and clinical workflows.

At Imprivata, our understanding of unique and complex healthcare workflows and IT systems has made us the world leader in trusted digital identity management for health delivery organizations. Our solutions are developed with — and vetted by — clinicians. It's how we're able to deliver frictionless interactions across the entire healthcare delivery ecosystem and why providers can focus on patient care, not technology.



References

Beazley Breach Briefing – 2019, March 21, 2019

“Delivering Frictionless Security to the Clinical Workflow: Access and Identity Management the Key to Workflow Efficiency,” Frost and Sullivan White Paper, Mike Jude, Ph.D.

“Experts at Johns Hopkins have calculated that more than 250,000 deaths per year are due to medical error in the United States,” Marty Makary, M.D., M.P.H., Study Questions Quality of U.S. Health Data, April 2015

“Healthcare IAM: Enhance the Clinical Workflow,” KuppingerCole, 2019

“Identity and Access Management Primer for 2019,” Gartner PDF

“Mahaska Health partnership saves clinicians 45 min/day with fast access to EMR applications,” Imprivata.com

“Medical Error” Carver N, Gupta V, Hipskind JE. February 16, 2020

“Report on Improving Health Care Industry Cybersecurity. Health Care Industry Cybersecurity Task Force”, June 2017, p.32

“The Unique Considerations for IAM in Healthcare,” Gus Malezis, President and Chief Executive Officer of Imprivata

“Using Health Informatics to Tackle Duplicate Medical Record Issues,” American Health Information Management Association, Shannon Harris, MBA, RHIA, and Shannon H. Houser, PhD, MPH, RHIA, FAHIMA

“Why digital identity is now a board-level topic,” KPMG



For more information, visit www.imprivata.com

© 2020 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.