TLP:WHITE

December 2023

# Health-ISAC: Biometrics & Healthcare

A Cure-all for Identity Woes?

Health-ISAC™
Collaborating for Resilience in Healthcare
SHARING SINCE 2010

health-isac.org

# Contents

# Scope Statement

It's been a decade since biometrics went mainstream. That's when Apple announced Touch ID, a fingerprint scanner embedded into iPhones used to access the device. Apple rolled out this functionality later to its laptops and iPads, and in intervening years, also introduced Face ID, which enabled access with a quick glance at a device using facial recognition.

Biometrics existed before 2013—other mobile device manufacturers had taken advantage of the verification technology in mobile devices prior to that—but its use was not widespread. But today, almost half of consumers use biometrics daily to access information on their mobile devices.[1] Biometrics have become ubiquitous as people use their face or finger to access their mobile device multiple times a day.

In the enterprise market, statistics around the use of biometrics are more difficult to find. Pockets of healthcare have started to utilize fingerprint, face, iris, and vein recognition for enterprise, physical, and patient access over the years, but use is still uneven across the sector.

Healthcare has several use cases that would be a great fit for biometrics with multi-factor authentication (MFA) for the caregiver and patient at the top of the list. This paper will look at biometric technologies—both physiological and behavioral—that can help healthcare organizations more easily enable MFA, secure patient data, and identity proof patients while also improving the experience for the healthcare provider and the patient.

[1] https://www.getapp.com/resources/biometric-technology/

## Key Takeaways

- Biometrics can help healthcare CISOs implement MFA.
- Physiological and behavioral biometrics are different, but each can help healthcare organizations.
- Not all biometrics systems work the same; some are more accurate than others, and some work better across a diverse population than others. Choosing solutions that work equitably across all populations is important, as is creating fallback solutions for times when biometrics may not work well for some people.
- The use of biometrics may present security and privacy considerations for both employee and patient use cases.
- Emerging threats from artificial intelligence are making the use of biometrics more complicated in some instances. Organizations needs to take a layered approach and not rely solely on biometrics for identity proofing or MFA.

## Biometrics defined

A decade ago, mention biometrics and most people thought about fingerprints. Now, people may think of a variety of technologies, including face recognition, iris, and voice. These are all **physiological** biometrics—they use physical traits to verify an individual.

There are also **behavioral** biometrics, which can analyze a user's keystrokes when typing, navigational patterns, screen pressure, typing speed, mouse or mobile movements, gyroscope position, and more. These technologies on their own may not provide enough information to positively verify an individual's identity, but layered together with other security technologies, they can go a long way while also improving the experience for the caregiver. As noted in Health-ISAC's previous paper, All About Authentication: A Health-ISAC Guide for CISOs,[2] behavioral biometrics are an essential component of delivering "continuous risk-based authentication" that integrates traditional MFA with signals from device analytics and behavioral biometrics.

[2] https://h-isac.org/wp-content/uploads/2021/02/H-ISAC_All-About-Authentication-White-Paper.pdf

The table below summarizes popular physiological and behavioral biometrics, the potential healthcare application where they can be used, and the pros/cons of that technology.

| Biometric Modality | Health Care Application | Pros | Cons |
|---|---|---|---|
| **Fingerprint** | Used for physical access to secure areas or medication dispensing equipment; also used with built-in sensors on laptops, phones, or tablets for access to applications and data. | Well-established technology that works well, easy to use, and inexpensive. | Caregivers are unable to authenticate when wearing gloves. May not work for people with thin or faint fingerprints. |
| **Face** | Used in conjunction with built-in cameras or separate webcams on devices to authenticate the individual. | Well-established technology that is often baked into many operating systems and applications. Also used in identity proofing to match the photo on the document to the individual presenting it. | Caregivers are often masked making authentication difficult. Lighting—too much or too little—can cause difficulty when authenticating. Certain algorithms or cameras may have difficulty with dark-skinned individuals. Deep fake technology using artificial intelligence has emerged that enables individuals to spoof this modality. |
| **Iris** | Used for access to secure areas and for dispensing medication. | Can be used when masked or gloved and at a distance. | Primarily used for physical access and not secure access to applications and data. |
| **Voice** | Used by caregivers and patients for authentication. Caregivers can authenticate via a simple phrase spoken into the device. Other healthcare organizations also use voice to authenticate patients dialing into call centers to verify identity. | Can be used with built-in microphones on all devices and doesn't require caregiver to remove mask or gloves. Provides additional layer of authentication for patient dialing into call center. | Background noise can interfere with authentication and new artificial intelligence (AI). Threats make it simple to copy someone's voice and present it as their own. |
| **Palm/Finger Vein** | Vein recognition uses infrared light to go beneath the skin and use an individual's unique palm, finger, or eye vein pattern to authenticate. | Vein recognition can be a contactless biometric and doesn't require a caregiver to remove their glove for authentication. Patient use cases exist for authentication at the point of care. | Technology can be proprietary and expensive. User experience can be difficult as individual needs to hold their hand a specific distance from the device. |
| **Behavioral biometrics** | Keystroke, mouse dynamics, screen dynamics, and signature are all examples of behavioral biometrics. They focus on the way an individual types, uses their mouse or trackpad, or patterns when using a tablet. These biometrics are often layered together. | Invisible to the individual using the device, systems are running in the background capturing information and forming a profile. | Enrollment can take time as the system needs to capture a certain amount of data to match against existing behavior. |

# The Killer App for Biometrics in Health Care: MFA

Of all of the places where biometrics can most easily help solve problems in healthcare, MFA is at the top of the list.

Compromised credentials are still a leading cause of data breaches, accounting for 61% of incidents.[3] Password sharing with shared workstations—a common occurrence in healthcare—is also problematic with 62% of workers reporting they have shared a password.[4]

Moreover, while the Health Insurance Portability and Accountability Act (HIPAA) regulations have traditionally not required MFA—only requiring the use of "strong passwords"—new June 2023 guidance from the Department of Health and Human Services (HHS)[5] states:

As a best practice, regulated entities should consider implementing multi-factor authentication solutions, including phishing-resistant multi-factor authentication, where appropriate to improve the security of ePHI and to best protect their information systems from cyber-attacks.

Additionally, the Drug Enforcement Agency provides several requirements related to MFA for administrators of prescribing systems, prescribers, and digital signing. Two-factor authentication must be used to enroll a prescriber within the electronic system, approve a prescription entry, and digitally sign a prescription.[6] Here, MFA possibilities include pairing a username and password with a security token, something you have, or biometric, something you are.

Exact numbers on MFA adoption in the healthcare market are difficult to come by, but it's typically been a tough market for the security technology. One of the biggest challenges has been in the caregiver setting, where the use of shared workstations has made deployment of some MFA tools difficult. Challenges include:

- **Tokens** – Having to remember to carry a token and plug it in (and remember to remove it from) a shared workstation or tablet can be cumbersome from a user experience perspective.

**62%**
of workers faced problems due to password sharing with shared workstations

**61%**
of data breaches are caused by compromised credentials

[3] https://www.verizon.com/business/resources/reports/dbir/
[4] https://www.keepersecurity.com/blog/2021/07/06/4-rules-for-safe-password-sharing-in-the-workplace/
[5] See June 2023 OCR Cybersecurity Newsletter at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html
[6] https://www.ecfr.gov/current/title-21/chapter-II/part-1311/subpart-C/section-1311.115

- **Near Field Communication** – Baked into mobile phones, this secure protocol enables individuals to tap and go for access to workstations. While sometimes better than tokens, NFC tools still require caregivers to be pulling out a mobile device and tapping it whenever they need access.
- **One Time Passwords (OTP)** – Caregivers don't want to stop what they're doing, pull their mobile device from a pocket, and enter a six-digit number every time they login to a system when caring for a patient.
- **Mobile push-based apps** – Same challenges as above but a slightly better user experience.
- **Biometrics** – Caregivers are often gloved and masked when caring for patients, making it difficult to use physical characteristics to verify an identity.

The easiest path to implementing MFA with biometrics is to adopt MFA that uses the FIDO Alliance standards, which pairs an on-device biometric match with a cryptographic key to deliver single-gesture MFA. FIDO specifically limits the use of biometrics to on-device matching, mitigating the significant security and legal risks—which this paper will explore in more detail later—associated with systems that store or match biometrics in a centralized, networked system. FIDO standards also provide a sort of "abstraction layer," that allows different biometric modalities and devices to be interoperable within an organization while delivering a consistent layer of security.

*The easiest path to implementing MFA with biometrics is to adopt MFA that uses the FIDO Alliance standards, which pairs an on-device biometric match with a cryptographic key to deliver single-gesture MFA.*

Notably, the updated June 2023 HHS guidance on MFA specifically advises organizations to use FIDO authentication because it is phishing-resistant, whereas other legacy MFA modalities like OTPs and push-based apps are not. Per the HHS advisory:

An example of phishing resistant multi-factor authentication would require a password or user biometric data coupled with a phishing resistant authenticator such as a Personal Identity Verification (PIV) card or other cryptographic hardware or software-based token authenticator (e.g., Fast Identity Online (FIDO) with WebAuthn authenticator). The layered defense of a properly implemented multi-factor authentication solution is stronger than single factor authentication such as relying on a password alone.

While there are difficulties with using traditional MFA modalities in healthcare, there are still options. Behavioral biometrics with other security technologies layered in can provide robust authentication technologies for healthcare workers to authenticate to secure systems.

**For a deeper dive into FIDO and other types of MFA, please see Health-ISAC's previous paper, All About Authentication: A Health-ISAC Guide for CISOs,[7]**

[7] https://h-isac.org/wp-content/uploads/2021/02/H-ISAC_All-About-Authentication-White-Paper.pdf

# Enterprise Biometric Use Cases

Below are use cases for enterprise and patient biometrics.

### Biometrics for physical access to pharmaceuticals

Jane is a nurse on a post-operative floor at a hospital. Prior to making her patient rounds, she visits the medication cabinet on the floor. She swipes her badge on the reader of the cabinet and then presents her previously enrolled finger to prove she is the rightful owner of the card. From there, she gathers the medication needed based on her patient list.

### Biometrics for MFA and access at the point of care.

Jane is making rounds to check on patients and administer medication. The hospital has computers on wheeled carts that nurses and physicians use to enter information into electronic medical records (EHR) software and create new patient orders.

After visiting with patients, Jane goes back to the cart where she places a finger on a scanner to authenticate. From there, she enters the necessary information into the EHR, adds orders for prescriptions and testing, and is able to access all other appropriate applications.

### Biometrics for physical access to restricted areas

The quarantine ward at Jane's hospital has restricted access. In order to make sure only authorized employees can gain access, the institution has implemented iris biometric physical access control. Staff swipe their access card and then look at a mirror in a camera that matches the iris to previously enrolled templates.

### Biometrics for MFA for the back-office staff

John is a billing coordinator at the hospital and is responsible for reviewing billing statements for accuracy. He has to access multiple applications in his day-to-day responsibilities. When John first logs into the system, he touches a fingerprint scanner embedded into the workstation, enters a password, and has access to the necessary systems. In the background, behavioral biometrics are tracking his mouse movement, keystroke patterns, and other information, enabling continuous risk-based authentication. John will be prompted for additional authentication if something anomalous is detected.

# Patient Biometrics Use Cases

## Biometrics for identity verification at point of care

Alice arrives at her doctor's appointment and goes to reception to check in. She gives her name, and the receptionist asks her for government-issued identification and proof of insurance. After the identity documents are scanned into the medical records system, Alice is asked to hold her hand over a palm vein scanner. This enrolls her in the biometrics verification system so that on future visits, she just needs to hold her hand over the infrared scanner, and she is checked in for her appointment.

## Face biometrics with document verification for remote identity proofing

Bob lives in a rural area and is unable to take the time to drive the great distance to see a physician. He is offered the option to see a doctor via a telehealth visit. Before the visit, Bob needs to enroll in the telehealth system. He enters his name, address, date of birth, and insurance information. Bob is then asked to provide a government-issued identity document. He takes a picture of the front and back of the document with his laptop camera or smartphone. He then also has to take a selfie that matches the photo on the document. Once that match is made and the other information is verified, Bob is enrolled into the telehealth system and the biometrics information used for enrollment is deleted.

## Voice biometrics for identity verification in call center

Janice is traveling for work and needs to change the address of where her medication is shipped. She calls her pharmacy benefits manager (PBM) to request a change of address for the shipment. Since Janice has called into the PBM before, she was enrolled in the voice biometrics verification system. As she's relaying information to the PBM, her voice is verified, and no other verification is necessary other than the operator asking for name, address, and other demographic data.

# Equity and bias considerations with biometrics

Not all biometrics systems work the same; some are more accurate than others, and some work better across a diverse population than others. Independent testing has shown that there is a material gap in performance between top tier systems and laggards.

For example, certain facial recognition systems have difficulty identifying and enrolling dark-skinned individuals; others struggle more with women than men. Organizations deploying face recognition should verify that they are using an algorithm that has been evaluated by the National Institute of Standards and Technology (NIST) and that it has been proven to perform well for all ethnicities, sexes, and skin tones.

Likewise, some biometrics can prove difficult to use for those with disabilities. Organizations implementing biometric technologies need to have alternative authentication mechanisms available in case individuals are not able to enroll or authenticate or provide assistive technology that can address usability challenges.

While facial biometrics have gotten the most attention here, other biometric modalities may also present challenges. For example:

- Some fingerprint algorithms have difficulty enrolling and authenticating individuals with exceptionally fine fingerprints. Other fallback authentication mechanisms should be offered in case this happens.
- Non-verbal individuals will not be able to use voice biometrics, so additional steps will be necessary for this population.

# Biometric Security and Privacy Considerations

As part of the biometric evaluation process, organizations should also review any applicable laws and regulations that could impact use of the technology and consider how employees and patients will receive the technology.

For example, in Illinois, the Biometrics Information Privacy Act regulates the collection, use, and handling of biometric identifiers and information by private entities. Private companies are prohibited from collecting biometrics unless they[8]:

- Inform in writing what data is being collected or stored.
- Inform the person in writing of the purpose for collection and length of time the data will be stored and used.

Obtain the individual’s written consent to use the information.

[8] https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa

Even if a state or local government does not have any laws or regulations around biometrics, taking the above steps is a best practice. Enabling employees to know what data is stored, how it is being used, and how long it will be stored gives them greater transparency.

Another critical security and privacy consideration to consider is where the biometric information will be stored and matched.[9] Some biometric authentication systems are architected to store and match biometrics locally; others are designed to store and match in central databases. There are also hybrid systems where biometrics may be stored and matched in multiple places.

While it may be tempting to store biometrics centrally, databases of biometric information come with risk, as they become targets and threaten the integrity of the system, as well as the security and privacy of the people whose data is stored. One challenge with biometrics is that they are not a secret. Unlike passwords or security tokens, once stolen, they can never be revoked or replaced. For this reason, the risks involved with the compromise of a central biometric data store—even in the cloud—is quite high.

As with storage, central matching systems introduce additional risks around security and privacy, as they mean that biometrics must be exported from a device and transmitted to the central matching location in a secure manner. Moreover, central matching systems present privacy concerns, as they can make it easier for an entity to track someone with their biometric over time. In contrast, authentication solutions that limit storage of biometrics to the device that they are collected on mitigate the risk of scalable attacks, in that any successful attack requires that the attacker gains physical possession of the device. As we detail below, the best biometric implementations make it physically impossible to export biometric information outside of a device. For this reason, it is best practice to ensure that biometrics are protected on devices by storing them in a protected container that is isolated from the rest of the device or in trusted hardware, such as a Trusted Platform Module (TPM) chip.

As noted earlier, healthcare organizations should look at MFA biometrics that use the FIDO standards since FIDO specifically limits the use of biometrics to on-device matching, mitigating the significant security and legal risks associated with systems that store or match biometrics in a centralized, networked system.

Within an enterprise, however, biometrics may also be implemented via systems that centrally store and match the biometric. This is commonly found within the health sector at provider facilities where a patient-facing professional may be roaming across shared devices from location to location and has a need to quickly log in to multiple devices. The security and privacy risks of central-match systems can be mitigated by:

- Storing biometric templates instead of raw images.
- Placing additional security controls around this biometric information to protect it from compromise.
- Employing biometrics sensors with strong Presentation Attack Detection (PAD) capabilities to ensure that attempts to bypass biometric authentication with spoofed or counterfeit biometrics are not possible.

[9] https://cdn2.hubspot.net/hubfs/3821841/docs/Secure-Biometric-Authentication-Achieving-Trusted-Cloud-Services(3).pdf

# Emerging threats from AI

Get used to seeing the term "Deepfake." It refers to multimedia that has been synthetically created or manipulated using some form of artificial intelligence. This technology is being used to fool video systems, face recognition, and voice biometric systems. With access to short audio or video clips of a target, fraudsters can play back audio or video that looks and/or sounds like someone else.

This technology is not new but is easier to use with the emergence of various AI tools. The FBI, Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) issued new advice on deepfakes and stated that the emerging threat could present a cybersecurity challenge for many organizations.[10]

To counter the new threats, organizations need to consider implementing a number of technologies to detect determine the source of the media. These recommendations include:

- Real-time verification capabilities.
- Passive detection techniques.
- Protection of high priority officers and their communications.

# Next Steps

Healthcare organizations wanting to implement biometrics should take the following steps:

- Review existing local laws and regulations around biometrics to make sure deployment abides by any existing laws.
- Evaluate which biometrics might be best for different use cases.
- Create new policies to cover use, data retention, and consent of individuals who will be using the technology, as well as exceptions for populations that cannot easily use biometrics or for whom biometrics may not work well.
- Pilot technologies in small use cases to determine whether the technologies fulfill the requirements; only deploy technology enterprise-wide if the pilot goes well.
- Layer security technologies to counter the rising threat of deepfakes.

[10] https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF