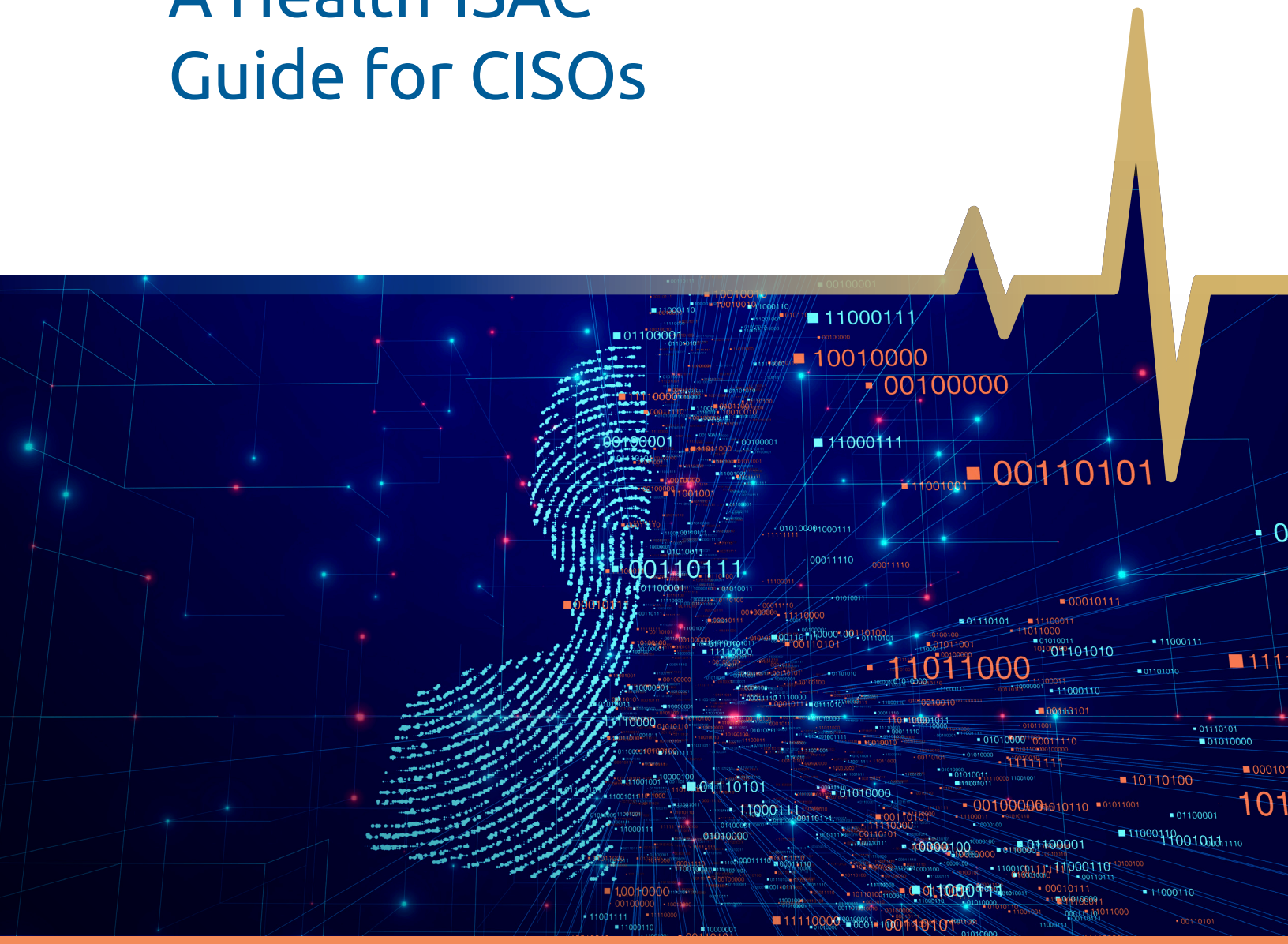
Remote Identity Proofing: A Health-ISAC Guide for CISOs



Health-ISAC™
Collaborating for Resilience in Healthcare
health-isac.org

Contents

Scope Statement

To put it bluntly, remote identity proofing is hard. For decades, organizations have been trying to come up with a reliable, secure, user-friendly way to make sure someone is not the proverbial "dog on the Internet." Despite many efforts, identity proofing is still one of the hardest problems to solve in the digital world.

In healthcare, identity proofing is a necessity to address a number of critical challenges, including preventing data breaches and ensuring electronic health records (EHR) are linked to the correct patient. Without a standardized approach across the health care ecosystem for remote identity proofing, organizations have cobbled together different products based on specific use cases to ensure the security of patient data, make sure they are receiving the right care and medication, and prevent fraud.

"On the Internet, nobody knows you're a dog."

Enabling interoperability across the health care ecosystem—providers, payors, and pharmacies—could envision a use case where a patient is proofed once and then that identity is used throughout the ecosystem. In a perfect scenario, health care providers would collect documentation from a patient during an in-office visit—scanning a government-issued identity document and validating insurance information—and attaching those attributes to a medical identity that can be used for telehealth visits, at pharmacies, and for access to medical record. However, in-person proofing is not always feasible, and there are many use cases where an in-person interaction is impractical. Here, remote identity proofing is the only option.

The purpose of this paper is to define common remote identity proofing approaches, explore how health care organizations can take a risk-based approach to remote identity proofing; and look at some current use cases and offer ways newer technologies can be used to offer greater security and usability.

Key Takeaways

- **Remote identity proofing is challenging** and offers attackers ample opportunities to exploit vulnerabilities to steal data and money
- **CISOs need to balance security and user experience** in crafting patient-facing remote identity proofing solutions.
- **Not all uses cases require the same level of assurance:** CISOs can take a risk-based approach to remote identity proofing that only requires a high assurance approach for high-risk use cases.
- **Not all uses cases require the same level of assurance.** CISOs can take a risk-based approach to remote identity proofing that only requires high-assurance approach for high-risk use cases.

Introduction

A patient visits the doctor's office and hands the receptionist a government-issued identity document and an insurance card. The receptionist scans those into the patient's record—sometimes also taking a photo—and then asks the patient to wait to be called. On the backend, the insurance information is validated, and as long as the name on the ID card is associated with the insurance information, everyone goes on their merry way.

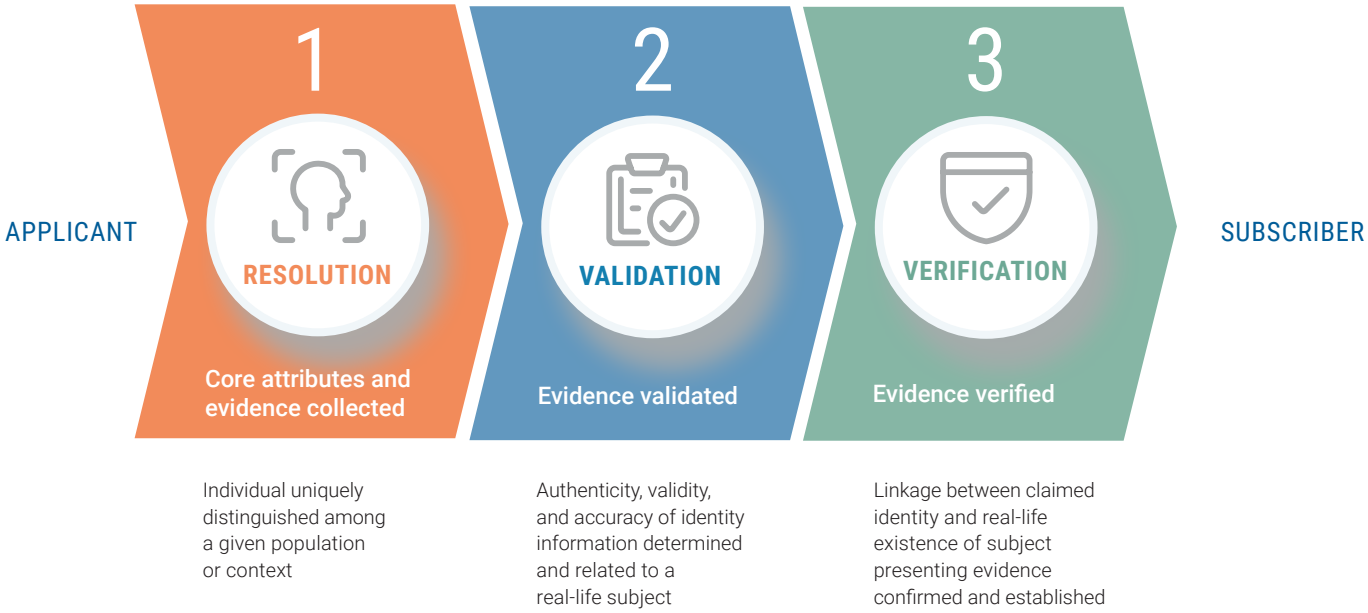
It is not as simple when an individual is dialing a call center or trying to enroll in an online system, since there is no driver license or state ID equivalent for these online situations. Authoritative data sources that link a flesh and blood individual to an actual identity are difficult to access and don't often exist in the online world. The alternative, which is what health care organizations have done, is patch together different tools that enable health care organizations to protect patient information and have some degree of assurance regarding who is accessing services and receiving care.

What is remote identity proofing?

Identity proofing is the process of proving your identity by either showing government-issued identity documents—in person—or in a variety of other ways remotely. Remote identity proofing in health care encompasses a few different use cases, mostly around online access to information and call centers. The focus of this paper is to explore current remote identity proofing options and the associated technologies in the context of the health care sector. While health care does have the potential to take advantage of in-person appointments to provision on-line accounts, we will also look at how organizations can take a risk based approach to remote proofing to save time and resources.

When it comes to identity proofing guidance a good place to start is the National Institute of Standards and Technology's (NIST) Digital Identity Guidelines Enrollment and Identity Proofing (Special Publication 800-63A).[1]

Figure 1: **The Identity Proofing User Journey Source: NIST SP 800-63A**



1 See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

These guidelines detail the expected outcomes from a proofed identity, including:

- Resolution of a claimed identity to a single, unique identity after attributes and evidence are collected, i.e., determining "of the 7,832 possible Linda Garcias that are in the U.S., which one is this?"
- Validation that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated), i.e., determining "that the documentation and information presented by 'Linda Garcia' is genuine."
- Proof that the claimed identity exists in the real world, i.e., determining that someone claiming to be a "particular Linda Garcia" is in fact a real person and not a made-up (aka synthetic) identity.
- Verification that the claimed identity is associated with the real person supplying the identity evidence, i.e., that someone claiming to be a "particular Linda Garcia" is in fact that person—and not someone who is trying to steal her identity.

NIST breaks down identity proofing into three categories, or Identity Assurance Levels (IALs):

Level	Description
IAL 1	Identity information is self-asserted, and no proofing takes place.
IAL 2	Evidence supports a real-world existence of the claimed identity and verification and validation that the applicant is associated with this real-world identity. Proofing can be done remotely or in person.
IAL 3	Physical presence is required for identity proofing and identifying attributes must be verified by an authorized and trained representative.

Health care organizations would typically only require identity proofing at IAL 2 for digital transactions, but providers have a path to IAL 3 with in-person touchpoints. At some point in a health care journey an individual is likely to show up to a health care provider in person. During that visit, most organizations have the ability to collect government-issued identity documents and other information. That information could then be used to create an online account backed by that in-person event. Health care workers would have to validate and verify the identity documents presented during an appointment, and then start the account creation process at that time. This last use case would be beyond what is currently being done, and health care organizations would have to make sure the proper security controls are put in place to protect the account—including multi-factor authentication (see "An H-ISAC Framework for CISOs to Manage Identity," April 2020).

Others in the health care ecosystem—payors and pharmacy benefits managers PBMs—are not as fortunate in that they do not see patients in person. However, the other IALs can fit those use cases. Accessing basic health care information—such as tips for managing high blood pressure or weight loss could be IAL 1. Accessing health records or prescription information online could use IAL 2. In-person transactions are fairly straightforward, it's the online use cases and technologies involved where it becomes more complicated.

Ultimately, remote identity proofing solutions present a number of challenges that need to be balanced to include:

- **Accuracy**: How to have assurance that an individual identity is valid
- **Security**: Preventing incidents tied to fraud, social engineering, or account take over
- **Usability**: Enabling access without forcing the patient to jump through so many hoops that they may abandon the transaction.

Identity Proofing Technologies

There are a number of technologies used to help organizations proof identities. While some are sold individually, most leading remote identity verification vendors will incorporate some or all of these technologies into a broader platform—looking at multiple signals to determine an individual's identity. The table below gives a sample of commonly used technologies, a description, relative strength, and challenges.

Technology	Description	Strength	Technology Challenge
Static Knowledge Based Verification (KBV)	Answers to questions that an individual provides when creating a new account, such as "street you grew up on" or "mother's maiden name." Can be used online and in call centers.	Weak	Answers to these questions are not secrets as they can easily be found on social media sites and as the results of the plethora of data breaches over the last 20 years.
Dynamic Knowledge-based Verification (KBV)	These "out-of-wallet" questions that are typically asked when opening up a new financial account, such as "which bank holds your mortgage?" or "which address did you live at in 1994?" Can be used online and in call centers.	Weak	Most of this information is also no longer secret due to data breaches. These questions can also pose some equity concerns, as not everyone has enough credit history or public information available to generate KBV questions.
Phone Verification/ Mobile Device Verification	These systems validate a number of attributes associated with a mobile device, including length of contract, if the number is being spoofed, if the device is new, and others. Can be used online and in call center.	Medium	Phone numbers can often be spoofed, and individuals that do not have mobile device contracts may show up as fraudsters in these systems.
Device/account verification	Verifies device and or account ownership by sending a one-time code to email or mobile phone to make sure the person calling in is actually the person who has possession of the account and mobile device. Can be used online and in call centers.	Medium	Has limited applicability with the mobile device verification and uses weaker email and SMS passcodes, which can be phished and are susceptible to other forms of hacking.
Facial Biometrics	Used in conjunction with document verification, this feature matches the individual's photo on the document with the person presenting it, including liveness detection to ensure that it's a legitimate person presenting it and not another photo.	Strong	The user experience with some of these systems can be challenging for some people and for those with older devices. The quality of some facial biometrics tools also varies—the best work accurately and equitably, but some second tier products do not.
Voice Biometrics	Voice biometrics is most commonly used in call centers to help verify the identity of an individual. It can also be used to support online use cases, though this is less common.	Strong	Capturing enrollment sample can be challenging; background noise can interfere with both enrollment and verification. Spoofing attacks with artificial intelligence software are also becoming more common.

Technology	Description	Strength	Technology Challenge
Risk-based scoring	These systems analyze various attributes about an individual that is either transacting online or via call center. The system will look at the device, operating system, serial number, IP address, geo-location, and various other metrics in the background to determine a potential fraud score.	Medium-to-Strong	Typically need to be used in conjunction with other identity proofing technologies to provide a holistic view of a patient.
Credential Service Provider (CSP)	If a patient has digital credentials at the IAL 2 or above from an approved CSP, it could be used for access to the health care organization's necessary resources.	Strong	Very few CSPs exist in the market, and the use of these credentials outside of government use cases are rare.

Health Care CISOs Should take a Risk-Based Approach to Identity Proofing

While organizations may be able to take advantage of in-person visits to connect the individual with an online account, health care CISOs should look at implementing a risk-based approach to remote identity proofing. The complexity of identity proofing requires multiple systems across call centers and websites to try and properly identify individuals wanting information and access. Trying to take a one-size-fits-all approach to identity proofing is not realistic; a risk-based approach allows CISOs to properly balance the three factors outlined above.

Risk-based remote identity proofing approaches often look at risk scores created by vendors that specialize in identity verification services. These scores are generally derived from various attributes about an individual—IP address, geolocation, device, and browser information, just to name a few. These risk engines run in the background analyzing various attributes to determine if something looks suspicious. If nothing from that score looks out of the ordinary the account can be created and little or no identity proofing will be required. If the risk score is higher the individual can be routed to another workflow with additional identity proofing that may include knowledge-based authentication, document verification with liveness and biometrics, or even dialing a call center.

Similar systems can be used in the call center. Fraud detection systems can monitor a variety of attributes from where the individual is calling from including the specific device. If it is the same number, with no signs of spoofing or other bad history, identity proofing can proceed. Overall, health care CISOs should look at their remote identity proofing processes to make sure the proper security controls are in place and evaluate whether the organization is doing enough, or maybe too much, when it comes to making sure someone isn't a "dog on the Internet."

Taking this approach can also save an organization money. Most of these systems charge on a per transaction basis, with document verification often being the costliest. By taking a risk-based approach and only having those individuals who meet a certain threshold on the risk score be asked to verify their identity documents or face, the organization can realize cost savings while also making it easier for the individual to create an account.

Below are some use cases for risk-based identity proofing in the health care ecosystem.

Use Case	Risk	Description	Risk-based Approach
General information	Low	An individual is searching for information about a doctor, medication, or health insurance information. In this instance no identity proofing is necessary and would just add friction for the individual looking for information.	None needed.
Marketing/ pricing information	Low	An individual is searching for information about a medication or high-level cost information for health insurance. In most instances no identity proofing is necessary for this use case, however, if an individual wants to receive an email with potential coupons for medication or quotes for health insurance based on general demographic data, IAL 1 with email verification would be appropriate.	Email address could be run through a risk engine to see if it's associated with fraudulent account.
Making an appointment	Low	This use case would require the individual to create an account and provide basic demographic information—name, address, date-of-birth, health insurance information—and the book an appointment.	Risk engine would look at the IP address and device information of the individual creating the account to see if there's any association with bad actors. If something suspicious is found the individual could be routed to a call center for additional proofing. Health insurance information would be validated on the backend and associated with the individual requesting the appointment. Additionally, once at the appointment, the individual will have their government-issued identity documents examined and scanned, bolstering the account to IAL 3 in the future.
Changing prescription information (online)	High	A patient accesses their pharmacy benefits manager (PBM) to change the shipping address for a critical medication.	Patient already has an account created and logs into the system to conduct the transaction. An OTP or FIDO authenticator is used for multifactor authentication. Risk engine identifies that transaction is being conducted from a typical, normal IP address and other attributes are validated as normal. If risk engine flags anything as suspicious the individual could be routed to a call center with a transaction code to notify the agent of the problem. The individual could also potentially be routed to a video call or document verification system to complete the transaction.
Changing prescription information (call center)	High	A patient calls the PBM to change the address for the next shipment of a critical medication.	Patient dials the PBM call center and requests the change of address. Risk engine checks the phone number and other data associated with it to ensure it's not fraudulent or spoofed. Individual's voice is verified against previous recording and transaction is processed. If a fraud flag was triggered, the individual could be asked to perform document verification via a mobile device or routed to a video call.

New Technologies for Remote Identity Proofing

Below we detail four health care-related scenarios where new technologies can help with remote identity proofing.

Scenario #1—Transfer of Personal Health Information

A patient calls their health care provider's call center to request that their electronic health record information be faxed to a specialist. The individual calling is from a different phone number than the one on record with the provider and the patient says they just recently changed numbers. However, the risk engine in place says that the number has been in use for years and has been associated with fraudulent calls in the past. The customer service representative requests various information from the patient—address, date of birth, insurance information—who has all the correct information. But because of the concern with the information from the risk engine, the representative asks for the specialist's name and phone number to validate that information independently before sending the health information.

Upon further investigation it was discovered that the individual calling was not the actual patient and was trying to access the individual's health information. In addition to the risk engine, a health care provider could also use voice biometrics that can help validate a patient's identity when conducting call center transactions.

Scenario #2—First time telehealth appointment

A patient has their first telehealth appointment with a physician. To set up the account the individual provided name, date of birth, email address, phone number, and health insurance information. The health insurance information is validated before the appointment and a risk engine checks IP address, email address, and other information to make sure nothing is suspicious.

At the time of the appointment the risk engine would once again check various data about the connection and device. Additionally, since this is the first appointment, the individual would undergo document verification. The patient would be asked to present a government-issued identity document to the camera. The information on the document would be checked against what was previously provided and security features would be verified to make sure the document is authentic. Lastly, the photo would be compared and matched to the individual presenting it.

If everything matches and the risk engine doesn't produce any red flags the patient would proceed with their appointment and their account would be validated with the identity information provided.

Scenario #3—First Time In-Person Appointment

A patient visits a health care provider for the first time and presents government identification—which is scanned and stored in the provider's EHR -- insurance information, and an email address at check in.

After the appointment, the patient goes home and finds an email asking them to create an account. The individual creates a username, password, and enrolls a multifactor modality—FIDO authenticator, push-based mobile app, or OTP as a second authentication factor. All of their information is already populated into the account due to the in-person visit. A risk engine also looks at the various attributes from where the individual is accessing the account and checks to make sure nothing is suspicious and makes a record that can be checked for future transactions

Scenario #4—PBM Call Center

A patient calls their PBM to request a change of address for a monthly prescription shipment. In this scenario, the individual already has gone through the account creation process, but their identity needs to be verified to make sure someone isn't trying to steal medication or find out what medication the individual is taking.

In this instance the individual recently purchased a new phone and had to change numbers so the information doesn't match what's on record. The customer service representative asks for name, date of birth, address, and insurance information. In the background the phone number the individual is calling from is run through a validation service that checks if it is a mobile or landline. Checks are also conducted to make sure the number is not being spoofed and for other information, such as how long the line has been active, if it is a mobile device, has it been used before, among other information checks.

Additionally, a voice biometric system has been in use by the PBM. Since the individual was previously enrolled their voice is matched against the enrolled template to verify the identity.

Because of the new phone number and device, the verification service can only do so much, but it does validate that the line and device are new. Fortunately, the voice biometric system is able to validate the voice print and verify the identity so the customer can complete the transaction.

Remote Identity Proofing Challenges

While technologies exist that can help health care organizations perform remote identity proofing and verification, challenges still exist. Many of them are around equity and inclusion, given a reliance on modern digital technologies like smartphones and broadband online technologies for individuals who may not have access to some resources.

For some with thin credit files and no public records data, they may not be able to generate a knowledge-based verification quiz. This would preclude them from registering an online account. Additionally, with the number of data breaches in the last two decades, much of the information that is in the quizzes is available to fraudsters, so this method alone should not be used for identity verification.

Mobile phone validation technology will not work very well for individuals that do not have a monthly plan or service in their name. For those with pay-as-you-go devices, these systems may throw up a false positive alert even though they are the correct individual.

Similar inclusion and equity concerns exist for document verification and biometrics. For some with older devices, capturing the document and facial match can be difficult because the technology is older. Likewise, these solutions may not work for some people with disabilities. Both of these factors may limit the ability of a single identity proofing solution to allow all people to successfully enroll. Facial recognition has also raised concerns around the ability to accurately enroll and match individuals with dark skin although NIST has stated that those biometric technologies that are most accurate are also generally the most equitable.

Because of these challenges, health care CISOs should look at taking advantage of in-person visits whenever possible to strengthen identity proofing.

Next Steps

Health care organizations should look at their current processes and evaluate where they can modify them. Additionally, they should:

- **Use in-person interactions to add high levels of assurance to online accounts and make sure proper security controls are in place for those online accounts.**
- **Inventory existing remote identity proofing technologies to determine full capabilities and if redundancies exist.**
- **Examine opportunities to implement risk-based identity proofing to ease friction on the individual and costs for the organization.**
- **As mobile Driver's Licenses (mDLs) emerge in many states—providing a digital counterpart to plastic ID cards—explore ways to replace legacy identity proofing components with capabilities that can tap into mDLs.**

New NIST draft changes IAL1

NIST released the draft of SP 800-63-4, *Digital Identity Guidelines*, in December 2022, which makes some changes to the previous Identity Assurance Levels (IALs).

In the previous version of SP 800-63, Enrollment *and Identity Proofing*, IAL 1 is a self-asserted identity. An individual could provide an email address, verify that email and they were IAL 1. Now IAL 1 requires the collection of:

- One piece of superior identity evidence—such as a valid passport
- Or one piece each of strong evidence—a driver license or permanent resident card—
- And a piece of fair evidence—a school ID card or financial account statement.

Biometric matching is optional at IAL 1, but identity evidence still needs to be verified and validated. Remote proofing is possible for both IAL 1 and 2. The requirements for IAL 2 and 3 did not change very much from the previous version of the guidelines.

However, additional requirements around equity have been added to the new draft. Credential Service Providers shall document the measures it takes to mitigate inequitable access and reassess equity concerns when adding new components and on a periodic basis. The goal is to make sure that identity proofing technologies work for everyone.

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at **contact@h-isac.org**