Center on Budget and Policy Priorities

1275 First Street NE, Suite 1200
Washington, DC 20002

Tel: 202-408-1080
Fax: 202-408-1056

center@cbpp.org
www.cbpp.org

August 27, 2024

Remote Identity Proofing: Better Solutions Needed to Ensure Equitable Access

By Symonne Singleton

Many Medicaid participants use an online portal to apply for the program and access their accounts. Some state Medicaid agencies require or prompt applicants to verify their identity, a process known as identity proofing, as part of securing online access.[1] Agencies may do this with the intention of protecting applicants' privacy and system security, as well as preventing identity or benefits theft. However, identity proofing can unnecessarily burden clients and prevent eligible people from accessing benefits. These burdens often fall heaviest on populations that are already marginalized, including people of color, people who are immigrants, and victims of identity theft.

In most cases, there is no federal requirement for state agencies to implement identity proofing in Medicaid, nonetheless about half of states do so anyway, and ten states require it for online applications.[2] Federal agencies such as the National Institute for Standards and Technology (NIST) and the White House have released guidelines and executive orders on customer experience that can help state agencies determine whether identity proofing is a useful tool for their user and IT needs.

The most recent federal guidelines place an increased focus on designing solutions rooted in usability and effectively meeting people's needs, while acknowledging rapidly evolving security needs. Using this design approach, also known as human-centered design, requires understanding the inequities in the current identity proofing process. Identity proofing may create roadblocks that prevent a person from applying for or accessing benefits. Also, identity proofing often relies on technologies that have significant shortcomings due to data breaches and well-documented racial bias. As a result, identity proofing often imposes unnecessary burdens on clients without guaranteeing a more technologically secure service.

While effective government services need to maintain security by assessing risks to clients and the government, agencies should consider whether identity proofing mitigates those risks and evaluate its potential negative impact on clients' access to benefits. In most cases, they will likely conclude that identity proofing should not be required for Medicaid applications.

[1] Jennifer Wagner and Genevieve Gaudet, "Removing Barriers to Access From Remote Identity Proofing," CBPP, April 22, 2020, https://www.cbpp.org/research/removing-barriers-to-access-from-remote-identity-proofing.

[2] Elizabeth Bynum Sorrell and Ariel Kennan, "Digital Authentication and Identity Proofing in MAGI Medicaid Applications," Digital Benefits Hub, May 19, 2023, https://www.digitalbenefitshub.org/publications/digital-authentication-and-identity-proofing-data/magi-medicaid.

Therefore, states that have not yet implemented identity proofing should defer until more accessible alternatives are available. States that have already implemented identity proofing should make it an optional step in the process and consider removing it in the future. In both cases, agencies can mitigate risk through other business practices, such as accessing available data sources to confirm identity. Striking the balance between security and ease of access will allow more applicants and enrollees to receive the public benefits to which they are entitled.

This paper explains the basics of identity proofing and how it relates to risk management. It then details how identity proofing can negatively impact Medicaid access and equity. It also highlights federal guidance and current business practices that support removing identity proofing as a barrier.

Background

The key terms and concepts involved in identity proofing include the following:

- **Identity proofing** (sometimes called identity verification) is a process by which an individual provides sufficient information to establish their digital identity, such as a username, password, documents, or personal identifiable information (PII) such as name, Social Security number, or date of birth.[3] Identity proofing can happen remotely or in person. If it occurs remotely, it is referred to as remote identity proofing (RIDP). Knowledge-based verification and biometric verification are two of the most common forms of RIDP.
- **Digital identity** is the online "persona" of someone using an online service, with a one-to-one relationship between a human and their digital presence.[4] If you have ever created an account online, you have interacted with a digital identity.
- **Authentication** is "the process of determining the validity of one or more authenticators used to claim a digital identity." [5] To cite a few examples, an authenticator could be something you *know* (e.g., a password or PIN), something you *have* (e.g., a one-time code sent to your phone), or something you *are* (e.g., a fingerprint).
- **Single sign-on (SSO)**[6] is an authentication method that allows users to use a single set of credentials, such as username and password, to access multiple applications. Agencies may employ SSO to allow a user to access multiple services. For example, once a person authenticates through a state SSO, they may be able to renew their driver's license, apply for a permit, and renew their Medicaid benefits, all with the same set of login credentials.
- **Knowledge-based verification (KBV)** is a form of RIDP in which users must answer multiple-choice questions based on private information associated with their identity, usually drawn from their credit history. These questions are sometimes referred to as "out of wallet"

[3] National Institute of Standards and Technology, "Glossary: identity proofing," https://csrc.nist.gov/glossary/term/identity_proofing.

[4] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, "Digital Identity Guidelines," National Institute of Standards and Technology, NIST Special Publication 800-63-3, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[5] David Temoshok *et al.,* "Digital Identity Guidelines Authentication and Authenticator Management," National Institute for Science and Technology, August 2024, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.2pd.pdf.

[6] Digital Benefits Network, Beeck Center for Social Impact and Innovation at Georgetown University, "Digital Identity Glossary," December 2022, https://www.digitalbenefitshub.org/resources/digital-identity-glossary.

questions because they should include information that couldn't be found from a stolen wallet. Common topics include past addresses, information about cars purchased, and former employers.

- **Biometric verification,** an alternative method of RIDP, is the use of "automated technologies for authenticating and verifying human body characteristics."[7] The most common forms of biometrics used for verification are facial features, fingerprints, iris patterns, and voiceprints.[8]
- **The NIST Digital Identity Guidelines** are considered the industry standard in the private sector and federal government for organizations establishing digital identity policies for users.[9] The guidelines were published in 2017 by the National Institute for Standards and Technology, an agency within the U.S. Department of Commerce that focuses on innovation, measurement, and development and use of standards. States are not required to follow the guidelines, although vendors and state agencies may use them as a reference or marketing point.

  The NIST Digital Identity Guidelines are evolving, with a particular focus on striking a balance between deterring fraud and advancing equity. KBV and biometrics raise specific concerns about effectiveness and equity, as explained below. NIST recently published a new version of the Digital Identity Guidelines in draft form for public comment.[10] This paper references both versions, as the 2017 version is used in the industry for current compliance and the updated version previews standards that should soon become the official standard.

Risk Management

Agencies can pursue the goals of identity proofing — ensuring security and preventing fraud — without the barriers that identity proofing can create by applying the principles of risk management. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.[11]

Assessing and Responding to Risk

A useful navigation tool for risk management is the "Digital Identity Risk Assessment Playbook," developed by a number of federal agencies, including the Centers for Medicare & Medicaid Services (CMS) and Department of Health and Human Services (HHS).[12] The playbook explores considerations around digital identity, including determining whether identity proofing may be necessary.

[7] National Institute of Standards and Technology, "Glossary: biometrics," https://csrc.nist.gov/glossary/term/biometrics.

[8] Biometrics Institute, "Types of Biometrics," https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

[9] Grassi, Garcia, and Fenton.

[10] David Temoshok *et al.,* "Digital Identity Guidelines: 2nd Public Draft," National Institute of Standards and Technology, NIST Special Publication 800-63-4, August 21, 2024, https://csrc.nist.gov/pubs/sp/800/63/4/2pd.

[11] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, September 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[12] Identity, Credential, and Access Management Subcommittee, "Digital Identity Risk Assessment Playbook, Version 1.2," December 29, 2022, https://www.idmanagement.gov/playbooks/dira/#step-2-identify-risks-and-assurance-levels.

Using the playbook, agencies can examine issues such as risk impact (in other words, what are the risks to this agency if you are not who you say you are?) and identity assurance (how sure is this agency that you are who you say you are?). Risk impacts are measured on a scale of low, moderate, and high and include financial loss, civil/criminal violations, and unauthorized release of sensitive information. Once an agency determines the risk impact, it can apply the proper identity assurance level. There are three such levels, with increasingly stringent identity verification methods and thus increasing confidence in the accuracy of the identity; identity proofing is not required at the lowest level.

CMS also has its own "Risk Management Handbook," which recommends that a risk assessment be conducted for CMS information systems as a collaborative process with multiple contributors. [13] Specifically, organizations should "conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards."

Although these playbooks and handbooks can help guide agencies' decision-making regarding identity proofing, agencies make their own determinations about risk and implementation. They should consider not only the security-related impacts of implementing, but also the potential impacts on users' ability to access the support they are entitled to.

Risks in Public Benefits: Identity Theft and Benefits Theft

When assessing risk within public benefit programs such as Medicaid, there are two primary concerns: identity theft and benefits theft. Identity theft occurs when "someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."[14] For example, someone could gain unauthorized access to another person's Social Security number and use that information for fraudulent activity. Identity proofing is not particularly helpful in mitigating identity theft, which is better addressed through robust authentication of online accounts.

Benefits theft occurs when a person receives public benefits for which they do not qualify. There are two main types of benefits theft. The first occurs when an applicant for benefits uses their own identity but inaccurately reports eligibility information, such as income or household size. Identity proofing would not prevent this type of benefits theft because the applicant is who they say they are. Instead, such discrepancies would be addressed through procedures during the application process, such as consulting data sources. The second type of benefits theft occurs when a person applies for benefits using the identity of another person who qualifies for benefits. Identity proofing may be helpful in mitigating this type of benefits theft.

The risk of benefits theft varies significantly from program to program, largely depending on the type of benefit provided. Programs such as Medicaid provide access to health care, not cash-like aid, so there is much less risk of benefits theft during application. (Medicaid measures other types of

[13] Centers for Medicare & Medicaid Services, Information Security and Privacy Group, "Risk Management Handbook Chapter 14: Risk Assessment," October 19, 2018, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-14-Risk-Assessment.pdf.

[14] Criminal Division, U.S. Department of Justice, "Identity Theft," August 11, 2023, https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

fraud through each state's Medicaid Fraud Control Unit, but their focus is on the larger issue of provider fraud.)

Regardless of the program, the possible risks of theft must be balanced with ensuring equitable access to benefits. Often, identity proofing is unnecessary because other business processes can address concerns around benefits and identity theft.

Digital Identity in Medicaid Eligibility and Enrollment

Individuals who apply for Medicaid on paper are not required to perform identity proofing. According to CMS guidance, paper applications must only require that "the adult application filer will sign his or her name under penalty of perjury, which is sufficient to enable the Marketplace, state Medicaid agency, or state CHIP agency to adjudicate the application."[15] Online applications should be held to the same standard until there is a better form of identity proofing that does not impose administrative burden. Even in states that do include some identity proofing, it can be made entirely optional, as is the case for more than half of the agencies that currently implement RIDP for Medicaid.[16]

There is one circumstance where CMS currently requires identity proofing with Medicaid applications.[17] If an online portal displays information obtained from confidential state or federal data sources directly to the applicant, as some Medicaid applications that are integrated with state-based marketplace applications do, identity proofing is required before application.[18] Ideally, these states would rework their systems to not send confidential information back to applicants, removing any need for meeting this requirement.

Beyond this requirement, RIDP is not a necessary tool for agencies to address fraud. Nor is it the most effective. In fact, even without RIDP, Medicaid clients confirm their identity on an application multiple times. They often submit information such as their Social Security number, date of birth, and pay stubs or other financial information. This information is checked against data sources and used to confirm the identity and eligibility of a person applying for benefits. Duplicating the confirmation of identity through RIDP is inefficient and creates additional burden for applicants and agencies.

Unnecessary RIDP is a form of administrative burden. Public program administrative burdens, or the costs associated with participating in government benefits and services, "can be a significant obstacle to individuals accessing support to which they are entitled," according to the Office of

[15] Centers for Medicare & Medicaid Services, "Guidance Regarding Identity Proofing for the Marketplace, Medicaid, and CHIP, and the Disclosure of Certain Data Obtained through the Data Services Hub," June 11, 2013, https://hbex.coveredca.com/regulations/PDFs/CMS%20FAQ%20-%20Guidance%20Regarding%20Identity%20Proofing.pdf.

[16] Bynum Sorrell and Kennan.

[17] Department of Health and Human Services, "Computer Matching Agreement Between Department of Health and Human Services, Centers for Medicare & Medicaid Services, and State-Based Administering Entities for Determining Eligibility for Enrollment in Applicable State Health Subsidy Programs Under the Patient Protection and Affordable Care Act," Attachment C, June 11, 2013, https://www.hhs.gov/sites/default/files/cma-1601.pdf.

[18] Centers for Medicare & Medicaid Services, "Guidance Regarding Identity Proofing for the Marketplace, Medicaid, and CHIP, and the Disclosure of Certain Data Obtained through the Data Services Hub," June 11, 2013, https://hbex.coveredca.com/regulations/PDFs/CMS%20FAQ%20-%20Guidance%20Regarding%20Identity%20Proofing.pdf.

Management and Budget.[19] Administrative burden often falls disproportionately on already marginalized populations and may deter applicants from accessing much-needed services or prevent them from retaining benefits for which they're eligible.

Inequity in Knowledge-Based Verification

Requiring identity proofing, especially knowledge-based verification, presents a significant barrier to entry for applicants, particularly those from historically underserved groups. Examples of information requested in KBV questions include past addresses, mortgage details, credit card accounts, and schools attended. (The precise information requested is largely dependent on information provided by credit reporting agencies.) Some individuals applying for benefits programs like Medicaid may have limited or no credit history and therefore be unable to complete KBV and be blocked from accessing online services. People who are immigrants, young people, and victims of identity fraud are among those who could face substantial challenges when completing KBV in the remote identity proofing process.[20]

It is the responsibility of agencies to address the needs of these clients, many of whom experience compounding inequities at several points in the application and enrollment processes. As the revised NIST guidelines explain, clients from these groups may be:

> unable to successfully present a digital identity or face a higher degree of burden in navigating online services than their more privileged peers. In a public service context, this poses a direct risk to successful mission delivery. In a broader societal context, challenges related to digital access can exacerbate existing inequities and continue systemic cycles of exclusion for historically marginalized and underserved groups.[21]

Security Concerns in Knowledge-Based Verification

A 2019 Government Accountability Office (GAO) study on the online identity verification process not only raised the inequity concerns listed above, but also found that large-scale data breaches have made KBV a far less secure and effective tool.[22] Equifax, one of the nation's three largest credit bureaus, had a major data breach in 2017 that exposed the personal information of approximately 147 million people, including "names, home addresses, phone number, dates of birth, social security numbers, and driver's license numbers."[23] Because KBV questions are based on this kind of information, the data stolen could be used to fraudulently answer KBV questions. GAO recommended that NIST provide guidance on implementing alternatives to KBV, given concerns about security and client burdens. According to updates from this study, NIST has issued additional guidance and implementation resources to assist agencies with alternatives to KBV.

[19] Office of Management and Budget - Office of Information and Regulatory Affairs Memo, "Strategies for Reducing Administrative Burden in Public Benefit and Service Programs," December 2022, https://www.whitehouse.gov/wp-content/uploads/2022/12/BurdenReductionStrategies.pdf.

[20] Terri Shaw and Shelby Gonzales, "Remote Identity Proofing: Impacts on Access to Health Insurance," CBPP, January 7, 2016, https://www.cbpp.org/research/health/remote-identity-proofing-impacts-on-access-to-health-insurance.

[21] Temoshok *et al.,* "Digital Identity Guidelines: 2nd Public Draft."

[22] U.S. Government Accountability Office, "Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes," June 14, 2019, https://www.gao.gov/products/gao-19-288.

[23] Electronic Privacy Information Center, "Equifax Data Breach," https://archive.epic.org/privacy/data-breach/equifax/.

Consequences of Unsuccessful Knowledge-Based Verification

In some cases, if a Medicaid system user cannot complete a required RIDP step, agencies do not provide additional support remotely. This is most common when people are applying through the federally facilitated marketplace, but it can also occur when applying for Medicaid through a state portal.[24] With no troubleshooting support from the agency, the applicant must contact the RIDP service (e.g., Equifax) directly.[25] The RIDP service then walks the client through often-repetitive steps to attempt to confirm their identity. If that alternative fails, the applicant cannot access the online system until they successfully prove their identity in person.

If a client does not have a credit history, has had their identity stolen, or cannot remember the information needed to answer the KBV questions, they will not be able to complete RIDP and, in turn, will not be able to apply or access their own portal. This not only harms clients but also leads to increased calls or visits to agencies, resulting in longer wait times and additional tasks for call center caseworkers.[26] According to one advocate in Kentucky:

> This process is a huge barrier for several reasons. We know how hard it is to set up an account in the first place, and if a person doesn't have reliable internet access, or isn't particularly technologically savvy, or has any kind of cognitive impairment, this process would be difficult to complete. If a person does not have credit, then completing the identity proofing becomes even more difficult — requiring transportation, and the time to sit and wait for answers, and then repeat that process when the answer is that you have to go somewhere else.[27]

Inequity in Biometric Verification

Biometric verification, the current alternative to knowledge-based verification, is arguably the more harmful option of the two. There are significant concerns about the effectiveness of biometrics and its impact on privacy and equity, especially for marginalized populations.[28]

Biometrics, particularly facial recognition, suffers from high error rates that reflect severe racial bias.[29] A 2018 study by Joy Buolamwini from the MIT Media Lab found that the error rates for facial recognition of darker-skinned females were up to 34 percent higher than for lighter-skinned males.[30] NIST confirmed this bias in an independent assessment, which found that across a total of

[24] Beyond the Basics, "Troubleshooting Failed Identity Verification on HealthCare.gov," September 2023, https://www.healthreformbeyondthebasics.org/troubleshooting-id-verification/.

[25] Centers for Medicare & Medicaid Services, "Questions and Answers about Remote Identity Proofing and Multi-Factor Authentication," October 2015, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Downloads/HETSHPGRIDPMFAFAQ.pdf.

[26] CBPP, "Unwinding Watch: Tracking Medicaid Coverage as Pandemic Protections End," November 30, 2023, https://www.cbpp.org/research/health/unwinding-watch-tracking-medicaid-coverage-as-pandemic-protections-end#:~:text=Coupled%20with%20large%20renewal%20backlogs%2C%20the%20August,20%20minutes%20or%20higher%20in%2011%20states.

[27] Holly Hudnall, Kentucky Voices for Health, in conversation with Code for America, August 2023.

[28] Hannah Quay-de la Vallee, "Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives," Center for Democracy and Technology, June 7, 2022, https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/.

[29] Alex Najibi, "Racial Discrimination in Face Recognition Technology," Science in the News, October 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[30] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research,* 2018, https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

189 facial recognition algorithms, every single one was least accurate in recognizing women of color.[31]

Beyond the "coded bias"[32] of biometric technology, users may associate the collection of biometrics with government surveillance. Facial recognition and other surveillance tools are often used to target majority Black and immigrant communities in policing. Including biometrics in a public benefits application can significantly deter people from accessing benefits by reaffirming their distrust of government agencies.

Inequity in Single Sign-On

Although SSO may have benefits in streamlining access and account management, it can lead to unnecessary identity proofing that blocks applicants from accessing services. Because SSO uses a single protocol across programs and services, if one of the applications accessed through an SSO requires RIDP, *all* applications under that SSO may then require RIDP. In the case of Medicaid applications, it is beneficial to allow clients to apply without having to sign in, meaning SSO might be a bad fit for this program.

Guidance on Equity in Identity Proofing

The revised NIST Digital Identity Guidelines place significant emphasis on optionality and choice for customers, particularly encouraging methods other than biometric facial recognition technology and knowledge-based verification. The guidelines explain that during identity proofing implementation, organizations should consider:

> how digital identity decisions that prioritize security might affect, or need to accommodate, the individuals who interact with the organization's programs and services. Privacy, equity, and usability for individuals should be considered along with security. Additionally, organizations should consider their digital identity approach alongside other mechanisms for identity management, such as those used in call centers and in-person interactions. By taking a humancentric and continuously informed approach to mission delivery, organizations have an opportunity to incrementally build trust with the variety of populations they serve, improve customer satisfaction, identify issues more quickly, and provide individuals with culturally appropriate and effective redress options.[33]

In addition to the NIST Guidelines, the Biden Administration released two executive orders in 2021 that can influence agencies' decision making around RIDP. One, on transforming the federal customer experience and service delivery, explains that every interaction with the government, including applying for benefits, is an opportunity to demonstrate that the government understands

[31] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test Part 3: Demographic Effects," National Institute of Standards and Technology, NISTIR 8280, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[32] "Coded Bias," a documentary released in 2020, "explores the fallout of MIT Media Lab researcher Joy Buolamwini's discovery that facial recognition does not see dark-skinned faces accurately, and her journey to push for the first-ever legislation in the U.S. to govern against bias in the algorithms that impact us all." See https://www.codedbias.com/.

[33] Temoshok *et al.,* "Digital Identity Guidelines: 2nd Public Draft."

and is responsive to users' needs.[34] The other, on advancing racial equity and support for underserved communities, states that "the Federal Government should pursue a comprehensive approach to advancing equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality."[35] The White House has emphasized the importance of examining how requirements like RIDP impact the customer experience and racial equity when determining the effectiveness of identity proofing in public benefits.

Conclusion

Remote identity proofing will remain an important issue as agencies continue to expand online access to benefits applications and distribution. It is crucial that agencies balance concerns around theft with ensuring equitable and usable applications.

Agencies that do not currently use RIDP should resist implementing it, particularly given that industry standards like the NIST guidelines are shifting. Instead, agencies and clients would benefit from revisiting implementation once more equitable options become available. If an agency has already implemented RIDP, the identity proofing step should be optional.

Agencies that conduct a risk assessment and determine that RIDP may be required should pause to investigate which attributes of their online process pose the significant risk. Alternative approaches may be available that do not require identity proofing but allow the agency to communicate effectively with users without the risk of sharing sensitive information.

[34] White House, "Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government," December 13, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/.

[35] White House, "Executive Order On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," January 20, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/.