KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

October 7, 2024

RE: *Second Draft of Revisions to NIST Digital Identity Guidelines (SP 800-63-4)*

Submitted via email to: dig-comments@nist.gov.

Kaiser Permanente (KP) appreciates the opportunity to offer comments on the above-captioned request for comment.[1] The Kaiser Permanente Medical Care Program is the largest private integrated health care delivery system in the U.S., delivering health care to over 12 million members in eight states and the District of Columbia[2] and is committed to providing the highest quality health care.

The rapid proliferation of online services over the past few years, particularly in response to social and economic changes brought about by the pandemic, has increased the need for reliable, equitable, secure, and privacy-protective digital identity solutions. As a health care organization, Kaiser Permanente has a responsibility to protect our data and systems, as well as the data of our members and patients, from security threats and breaches. We appreciate efforts by NIST to update the suite of Digital Identity Guidelines offer the following in response to specific questions posed:

Risk Management and Identity Models

Is the "user controlled" wallet model sufficiently described to allow entities to understand its alignment to real-world implementations of wallet-based solutions such as mobile driver's licenses and verifiable credentials?

We agree that the alignment of wallet models is key to moving forward and find that the "user controlled" wallet model is sufficiently described.

Identity Proofing and Enrollment

Is the updated structure of the requirements around defined types of proofing sufficiently clear? Are the types sufficiently described?

[1] https://csrc.nist.gov/pubs/sp/800/63/4/2pd

[2] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc. and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 39 hospitals and over 720 other clinical facilities; and the Permanente Medical Groups, self-governed physician group practices that exclusively contract with Kaiser Foundation Health Plan and its health plan subsidiaries to meet the health needs of Kaiser Permanente's members.

We recommend that the revised structure (IAL1, IAL2, IAL3) be updated to provide additional guidance for each role description along with expected diligence in the identity proofing that is required or minimally accepted for each level (1-Low risk, 2-Medium risk, 3-High risk).

We appreciate that IAL-2 now allows for acceptance of mobile driver license (mDL) under the user-controlled wallet model as evidence. This change facilitates identify proofing at a higher level to accept both physical and remote evidence validation.

Are the added identity evidence validation and authenticity requirements and performance metrics realistic and achievable with existing technology capabilities?

We recommend that the identity evidence validation and authenticity requirements and performance metrics be updated to allow organizations to differentiate between internal (employee) and external users in order to apply reasonable and appropriate processes that comport with the different roles and uses. For example, as a health care organization KP must have processes applicable to employees as internal users along with member beneficiaries and patients as external users. Both user types need access to our systems and data, but for different purposes and functions which require different business processes and operations, subject to different regulatory compliance factors, and pose different risks to our organization. Further, privacy protections must be applied to all identity evidence that is submitted to or acquired by the credential service providers (CSP) in addition to all other parties in the identity proofing process to ensure the process is secure and the privacy of individuals is protected. SP 800-63A-4 2pd applies general privacy requirements to CSPs; we recommend that this section be explicitly applied to all other parties in the identity proofing process and included in the guidance.

OTHER THOUGHTS

We offer the following additional feedback and recommendations based revised updates to SP 800-63-4:

Risk Management and Assurance Level Selection

We support the revised Risk Management and Assurance Level Selection process.

Digital Evidence

We support including digital evidence (e.g. mDL and Verifiable Credentials) and note that US states are in various stages of providing mDL access to residents. Incorporating the use of digital evidence in the Digital Identity Guidance is a natural next step and will serve to prepare the industry for when mDL is fully launched across every state in the US. However, while normalizing the use of digital evidence is important, it should not become the sole type of evidence accepted over time due to efficiency.

Presentation of physical evidence should always remain an option to support the Digital Identity process.

Trusted Referee and Applicant Reference

We support including these two roles to support individuals through the identity proofing processes that might not otherwise be able to complete them. We recommend that NIST clarify that applicant references may hold a power of attorney relationship to the applicant, but an applicant reference is not an implication of power of attorney.

Biometric Performance

We support the updated biometric performance requirements for proofing and authentication and agree with NIST's categorization of biometric evidence for the higher-risk level of IAL3.

Phishing Resistant Controls

The current draft guidance in 800-63-4 2pd recommends phishing resistant options in authentication protocol for AAL2 and requires phishing resistant options at AAL3. However, Fig. 1 Summary of requirements by AAL (pg. 10 of 800-63B-4 2pd) states that "AAL2 phishing resistant is recommended; must be available". We recommend that NIST correct this figure to state "AAL2 phishing is recommended; ~~must~~ may be available" to align with the draft guidance and ensure that the requirement reflects the appropriate control for the AAL2 level.

Additionally, we recommend that NIST conduct a comparative review of all AALs and IALs to ensure that requirements do not conflict between the three levels. For example, biometric methods for verifying evidence are described in 800-63A-4 2pd in section 4.2.6.3. However, one of the approved methods for verifying *fair* evidence is the same as those for verifying *strong* and *superior* evidence. This means that either the evidence required for strong or *superior evidence* is too low or the evidence required for *fair* is too high. We recommend NIST consider these requirements after a comprehensive review and adjust accordingly.

Password Requirements

The guidance in Appendix A3 should align risk and appropriate password management with users, taking industry expectations and compliance requirements into account. NIST should review the list of Password verifiers in section 3.1.1.2 of SP 800-63B-4 2pd to ensure alignment with industry security standards and expectations. For example, numbers 5 and 6 on the list are listed as "shall not" be required, however this guidance creates conflict with widely implemented and required password practices.

***

Thank you for considering our feedback. If you have questions or concerns, please contact me at [redacted]

Sincerely,

Jamie Ferguson
Vice President, Health IT Strategy and Policy
Kaiser Foundation Health Plan, Inc.