California Health & Human Services Data Exchange Framework

Strategy for Digital Identities

July 1, 2022

Table of Contents

Table of Tables

Version History

Date	Author	Comments
July 1, 2022	CalHHS CDII	Initial published version

Executive Summary

The California Health and Human Services Agency (CalHHS) completed the Strategy for Digital Identities to accompany the description of the Data Exchange Framework and the Data Sharing Agreement in partial fulfilment of the requirements of Assembly Bill 133. The Strategy was developed through critical consideration of recommendations gathered from Focus Groups representing stakeholder perspectives on digital identities and input from the Stakeholder Advisory Group, the Data Sharing Agreement Subcommittee, and public comment.

CalHHS considered a number of factors in drafting this strategy. Key among them were:

1. Meeting the requirements of AB-133 to "develop… a strategy for unique, secure digital identities capable of supporting master patient indices to be implemented by both private and public organizations in California."
2. Adopting consumer privacy as a key component of the Strategy, in addition to security as identified in AB-133.
3. Addressing the gap identified by the Stakeholder Advisory Group that "coordinated person identity matching services are needed to improve effective exchange of health and social services information."
4. Engaging stakeholders through consultation with the Stakeholder Advisory Group; convening Focus Groups to capture recommendations of diverse stakeholder experts; discussions with the Data Sharing Agreement Subcommittee; and public comment.
5. Applying the Guiding Principles developed for the Data Exchange Framework in consultation with the Stakeholder Advisory Group.
6. Drawing on the experience and success of health information exchange and interoperability already present in California.
7. Considering the progress of national initiatives, state health information exchange, national networks, and national interoperability frameworks, and the investments of many California stakeholders and state agencies in digital identities.

See:

- Gap Identified by the Stakeholder Advisory Group for a discussion of the gap identified by the Stakeholder Advisory Group this Strategy begins to address;
- Definitions for a Strategy for Digital Identities for a definition of digital identities used in this Strategy;
- Process for Developing a Strategy for Digital Identities for a discussion of the process by which this Strategy was created; and
- Table 1 within Application of Guiding Principles for a discussion of how the Guiding Principles developed in collaboration with the Stakeholder Advisory Group were used in creating this strategy.

The Strategy for Digital Identities comprises two primary parts:

1. A discussion of the Attributes Included in a Digital Identity to be used for person matching and record linking; and
2. The potential for a Statewide Person Index that uses these attributes to coordinate person matching among participants of the Data Exchange Framework statewide.

Within this document, key characteristics of the Strategy for Digital Identities are highlighted in a call-out box with discussion of the characteristic and specific Strategy recommendations following. The characteristics of this Strategy for Digital Identities include:

General Characteristics

1. The purpose and use case proposed for digital identities is to associate accessed or exchanged health and social services information with the correct real person. This purpose includes person matching and record linking.

Characteristics of Attributes of Digital Identities

2. Digital identities include as attributes selected "Patient Demographics" data elements from the United States Core Data for Interoperability (USCDI) Version 2. These attributes include
   - name(s)
   - date of birth
   - gender (if required by a technical standard or regulation)
   - address(es)
   - phone number(s)
   - email address(es).
3. Digital identities include as additional attributes selected identifiers that are uniquely associated with one and only one real person, but only if related to health care services delivery. Examples of these attributes are
   - medical record numbers in electronic health records
   - health plan member identifiers.
4. Digital identities adopt standard formats and datasets for person demographics specified in United States Core Data for Interoperability (USCDI) Version 2.
5. Digital identities may also adopt standard formats and datasets other than USCDI promoted by federal initiatives and identified for use by the Data Exchange Framework. The US@ Project specifications should be used to inform the address attribute as USCDI does not call out a specific format for that data element.
6. A public and transparent process may develop additional required formats and datasets for use by the Data Exchange Framework where gaps in nationally-recognized standards exist.

---

7. A future version of the Strategy may consider adopting tokenization of unique identifiers within digital identities to reduce the threat of identity theft.

Characteristics of a Statewide Person Index

8. The Data Exchange Framework should include a statewide person index if funding can be identified and a sustainability plan can be developed.
9. Organizations participating in the Data Exchange Framework would be required to follow the same security and privacy requirements for digital identities as those afforded to health information by provisions in the Data Sharing Agreement.
10. The use of digital identities obtained via a statewide person index would be limited in the Data Sharing Agreement to linking health and social services information to a real person; that is person matching when accessing or exchanging information at an organization participating in Data Exchange Network exchange.
11. A plan for a statewide person index should explore how to involve consumers in accessing, contributing to, and/or managing their digital identities.
12. A plan for a statewide person index should explore the use of tokenization as an expanded service of a statewide person index.

See:

- Purpose for a definition of the purpose for digital identities as proposed by this Strategy;
- Table 2 for a listing and Attributes Included in a Digital Identity for a discussion of the attributes that are and are not proposed by this Strategy for inclusion in a digital identity;
- Standards for Attributes in a Digital Identity for a discussion of the technical standards for content and format proposed by this Strategy for attributes of a digital identity, comprising USCDI v2, other nationally-recognized guidelines or standards, and additional guidelines developed as necessary through a public and transparent process to fill gaps;
- Statewide Person Index for a discussion of a statewide person index proposed by this Strategy to coordinate person matching statewide;
- Potential Uses of a Statewide Person Index for a discussion of how the statewide person index might be used, including to provide some of the services of a record locator;
- Permitted Uses of a Statewide Person Index for a discussion of permitted uses proposed by this Strategy and which may be included in the Data Sharing Agreement, which would be limited to person matching and record linking; and
- Security and Privacy for a summary of the individual privacy considerations for digital identities and a statewide person index throughout this Strategy.

The Strategy for Digital Identities is intended as a working document. This initial version establishes a baseline for future considerations. As the Data Exchange Framework matures, CalHHS expects this strategy to mature as well through discussions with stakeholders in a public and transparent process.

Introduction and Background

On July 27, 2021, Governor Newsom signed Assembly Bill 133 (AB-133), enacting Health and Safety Code Division 109.7 Section 130290 and directing California Health and Human Services Agency (CalHHS) to establish a statewide California Health and Human Services Data Exchange Framework. AB-133 describes the Data Exchange Framework as a single data sharing agreement and common set of policies and procedures that will govern and require the exchange of health information among health care entities and government agencies in California.

AB-133 Requirement for a Strategy for Digital Identities

AB-133 also requires CalHHS, by July 31, 2022, to:

> *develop in consultation with the stakeholder advisory group… a strategy for unique, secure digital identities capable of supporting master patient indices to be implemented by both private and public organizations in California.*

This document describes an initial Strategy for Digital Identities, including the process by which the Strategy was developed, the purpose for digital identities within the Data Exchange Framework, what should comprise digital identities for the Data Exchange Framework, and the role of person indices. The Strategy for Digital Identities will continue to mature with and be informed by the Data Exchange Framework through a public and transparent process.

Gap Identified by the Stakeholder Advisory Group

The focus for the Strategy for Digital Identities was taken from a gap identified by the Stakeholder Advisory Group[1], namely that coordinated person identity matching services are needed to improve effective exchange of health and social services information.

Effective exchange and use of health and social services information is dependent upon linking records to the correct real person. Many health care providers, health plans, and data exchange intermediaries have robust person matching and record linking technologies within their organizations. However, the Stakeholder Advisory Group noted that there is no systematic coordination of digital identities, person matching, or record

[1] A roster for the Stakeholder Advisory Group can be found on CalHHS' Data Exchange Framework website.

linking across organizational boundaries in California, limiting the efficacy of cross-organizational data exchange.

As a result, organizations may:

- Fail to locate existing health or social services records that might exist within other organizations for individuals they serve, missing an opportunity to better inform a provider and to support care coordination and management
- Inappropriately link health or social services information from different organizations for different individuals to a single record, creating a confused and potentially dangerously misinformed picture of a person's care history or health and social services needs

This gap exists in large part because health and social services organizations' information systems fail to agree on a single "identity" for the individual.

California stakeholders have extensive experience in person matching and record linking through their own activities and through participation in existing networks. This experience was leveraged to help create a Strategy for Digital Identities. The Stakeholder Advisory Group agreed that the focus of the Strategy should be on linking health and social services information to the correct real person across organizational and sector boundaries.

> *Opportunity: Strategy for Digital Identities*
> *Summary: The state should adopt the Strategy for Digital Identities called for in AB 133 as a component of the Data Exchange Framework.*

Importantly, high-quality digital identities and successful person matching and record linking is not solved by technology alone. Organizations cannot rely solely on automated matching algorithms, but also require human action and intelligence to match (and importantly, not match) appropriate information when the results of technical and automated algorithms are uncertain or incomplete. This Strategy focuses on a technical definition of the attributes of a digital identity and technical services that may aid organizations in achieving successful person matching and record linking statewide. The implementation of identity services must also consider the limitations of technology and automation, and ensure sufficient human processes are included. Organizations that use digital identities and person matching services must be diligent in maintaining and improving the quality of digital identity attributes, and likewise account for sufficient human processes to ensure appropriate person matching and record linking.

See *Health Information Exchange in California: Gaps and Opportunities*[2] for more information on this and other gaps identified by the Stakeholder Advisory Group.

Definitions for a Strategy for Digital Identities

The following definitions were adopted by this Strategy to help focus discussions of the Stakeholder Advisory Group, digital identity Focus Groups, and Data Sharing Agreement Subcommittee, and to add needed detail to the requirement of AB-133:

> *a strategy for unique, secure digital identities capable of supporting master patient indices to be implemented by both private and public organizations in California.*

AB-133 calls for a strategy for digital identities.

Digital Identity is defined in this Strategy as the collection of attributes that establishes an identity associated with a real person in a specific context; in this case the context is for use on the Data Exchange Framework to exchange health and social services information.

AB-133 did not call for establishing a digital identifier, and a digital identity is not synonymous with a digital identifier. A digital identity may, but is not required to, include a digital credential such as a username and password that might be used by the real person to access their identity or their data.

AB-133 calls for digital identities to be unique and secure.

Unique Digital Identity is defined in this Strategy as a digital identity that uniquely identifies a specific real person and distinguishes that individual from all others.

Digital identities can be unique because they include an attribute unique to that individual (e.g., a login ID, an email address, an insurance ID number, or a social security number) or because attributes taken in combination identify a person uniquely (e.g., the individual's name, date of birth, address, and phone number).

Secure Digital Identity is defined in this Strategy as a digital identity that is protected against unauthorized access or modification, or intentional or unintentional loss or corruption.

Security for digital identities is critical when used in conjunction with access and exchange of health and social services information. Compromised digital identities

[2] See the *Data Exchange Framework: Gaps and Opportunities* on CalHHS' Data Exchange Framework website.

can result in identity theft and medical identity theft. The Data Sharing Agreement embodies security requirements for digital identities.

AB-133 does not call for digital identities to be private. However, Guiding Principles for the Data Exchange Framework, discussions of the Stakeholder Advisory Group, and deliberations of the Focus Groups quickly identified that privacy was a critical characteristic for digital identities.

Private Digital Identity is defined in this Strategy as a digital identity that is collected, used, and shared only in allowed ways for allowed purposes with organizations that have agreed to the privacy safeguards for digital identities and other data to protect personal privacy as specified in the Data Sharing Agreement and its Policies and Procedures.

The Data Sharing Agreement embodies privacy requirements for digital identities. This Strategy for Digital Identities extends privacy to identify those identity attributes that should not be collected or used for person matching and record linking purposes to protect individual confidentiality and increase consumer trust.

AB-133 calls for digital identities to support master patient indices. This document uses the term “person index” instead due to the larger potential use of the indices by social services organizations outside of a patient context. AB-133 does not call for a single, statewide person index, but instead for support of person indices that may be operated by organizations using the Data Exchange Framework.

Person Index is defined in this Strategy as a database or service that aggregates and cross-references digital identities across different organizations, systems, and contexts.

While a statewide person index is not a requirement of AB-133, Focus Group discussions supported the creation and operation of a statewide person index as the best way to facilitate and coordinate linking of health and social services information to the correct real person for access and exchange using the Data Exchange Framework.

This Strategy assumes that digital identities are “to be implemented by both private and public organizations”, but that AB-133 does not require implementation of a person index by any or all organizations. The Strategy includes considerations for organizations that do not implement or operate a person index.

Process for Developing a Strategy for Digital Identities

Development Process

Development of the Strategy for Digital Identities by CalHHS and the Center for Data Insights and Innovation (CDII) was guided by the requirements and deadlines set out by

AB-133 and was informed by extensive stakeholder engagement. It was also informed by development of the Data Exchange Framework and the Data Sharing Agreement and its associated Policies and Procedures.

Developing a robust and effective Strategy required input from industry experts representing public and private stakeholders potentially implicated by the Strategy's design and implementation. In addition to consultation with the Stakeholder Advisory Group as directed in AB-133, CalHHS convened a series of Focus Groups to capture diverse stakeholder perspectives, engaging over fifty strategic, technical, and operational experts inside and outside of California representing:[3]

- Health information exchange organizations
- Consumer privacy advocates
- Health care providers
- Health plans
- Social services organizations
- California state agencies and departments

The membership of each Focus Group drew most heavily from organizations based in or exchanging health or social services information in California. However, organizations outside of California were represented as well to ensure the discussions did not draw exclusively on California experience or ignore successes outside of California. Most notably, the health information exchange organization Focus Group included members from other states with experience in statewide digital identities, and the consumer privacy Focus Group included members of nationwide organizations for a broader representation of consumer privacy considerations and initiatives. Both the health care provider and health plan Focus Groups included members representing organizations that not only provided services in California but in other states as well.

The perspective of social services organizations may not be well-represented in this version of the Strategy for Digital Identities. Despite outreach to the Stakeholder Advisory Group and many social services organizations, very few social services organizations agreed to participate in a Focus Group due to a stated lack of expertise or time. A limited social services perspective was provided in the health information exchange organization Focus Group if the organization included social services organizations among their participants. As the data exchange among social services organizations and this Strategy matures, consideration should be given to improve representation of a social services perspective.

---

[3] Rosters for each Focus Group, and meeting materials and recordings of Focus Group meetings can be found on CalHHS' Data Exchange Framework website.

Each Focus Group met twice in public meetings from late January through March 2022. As CalHHS developed its Strategy for Digital Identities, it sought Focus Group and public feedback on:

- The purpose and use cases for digital identities within the Data Exchange Framework
- Elements of a digital identity that would enable more effective information exchange
- Standards for attributes of a digital identity
- The role of person indices and a potential statewide index
- Permitted use of digital identities and limitations on secondary use to protect privacy
- Barriers to adoption of a recommendations for a strategy for digital identities

High-level concepts used to develop the Strategy for Digital Identities and overarching questions were brought to the Stakeholder Advisory Group in its spring 2022 meetings for input. A draft Strategy was presented and discussed at the Stakeholder Advisory Group meeting on April 7, 2022. Comments and suggestions from the Stakeholder Advisory Group and other interested parties were sought, received, and incorporated into this document.

Key concepts regarding technical standards, security, and permitted uses of digital identities were also discussed with the Data Sharing Agreement Subcommittee[4] for inclusion in the Data Sharing Agreement and its associated Policies and Procedures. The Strategy for Digital Identities, while a separate product required by AB-133, is also cross-referenced in the Data Exchange Framework[5] and its Data Sharing Agreement and its associated Policies and Procedures.[6]

Finally, a public comment period was held to collect additional input from the public. The public comment period was also an opportunity for the Stakeholder Advisory Group and members of the Focus Groups to provide additional input on a full draft narrative of the

---

4 The Stakeholder Advisory Group convened the Data Sharing Agreement Subcommittee to focus on advising CalHHS and CDII while drafting the Data Sharing Agreement and its associated Policies and Procedures required by AB-133. A roster for the Data Sharing Agreement Subcommittee can be found on CalHHS' Data Exchange Framework website.

5 See the *Data Exchange Framework* on CalHHS' Data Exchange Framework website.

6 See the *Data Exchange Framework: Single Data Sharing Agreement* and associated Policies and Procedures on CalHHS' Data Exchange Framework website.

Strategy. Additionally, the public comment period was an opportunity for organizations not fully represented in the Focus Groups to provide input.

Application of Guiding Principles

The Data Exchange Framework Guiding Principles[7] establish the core expectations or "rules of the road" that guide the design and implementation of the Data Exchange Framework and the access and exchange of health and social services information in California.

Table 1 summarizes considerations and design activities for each of the Guiding Principles in developing the Strategy for Digital Identities for the Data Exchange Framework.

Table 1 Application of Guiding Principles for the Data Exchange Framework to the development of the Strategy for Digital Identities.

Guiding Principle	Considerations
1. Advance Health Equity 3. Support Whole Person Care	• Discussed how digital identities might be used to assess equity and access • Considered bidirectional use by both health and social services organizations
2. Make Data Available to Drive Decisions and Outcomes 7. Adhere to Data Exchange Standards	• Emphasized compatibility with federal standards
4. Promote Individual Data Access	• Considered identity needs to support consumer access
5. Reinforce Individual Data Privacy and Security 6. Establish Clear & Transparent Terms and Conditions 8. Ensure Accountability	• Discussed permitted uses, security (including with Data Sharing Agreement Subcommittee) • Considered privacy when identifying attributes

Advancing Health Equity and Support Whole Person Care: The Strategy for Digital Identities is designed to be used with both health care and social services

[7] See the *Data Exchange Framework: Guiding Principles* on CalHHS' Data Exchange Framework website.

organizations in mind. It anticipates bidirectional access and exchange of health and social services information by these organizations for whole-person care within the Data Exchange Framework and as allowed by the Data Sharing Agreement. Focus Group discussions specifically considered how digital identities might be used to assess equity and access to health care and social services.

Make Data Available to Drive Decisions and Outcomes and Adhere to Data Exchange Standards: Focus Group discussions emphasized the use of nationally-recognized technical standards and considered the level of adoption of those standards. Use of nationally-recognized standards allows the Strategy to align with national initiatives. Use of widely-adopted standards allows the Strategy to take advantage of current implementations and increases data availability. The Strategy for Digital Identities utilizes widely-adopted and nationally-recognized standards wherever possible.

Promote Individual Data Access: The Strategy for Digital Identities focuses on ensuring that accessed and exchanged information is appropriately linked to the correct real person. While digital identities may initially be used most often by health and social services organizations, appropriate record linking is fundamental to supporting individual access as well.

Reinforce Individual Data Privacy and Security, Establish Clear & Transparent Terms and Conditions, and Ensure Accountability: Discussions in all Focus Groups considered individual privacy and information security, and the need for health and social services organizations to be responsible and accountable in their collection and use of digital identity attributes. One Focus Group was identified specifically with individual privacy in mind. The Strategy for Digital Identities, its allowed purposes for use, and its privacy and security requirements are designed to balance the safety needs of proper individual identification with the privacy of individuals. The Strategy is intended to weigh privacy most heavily in most situations.

See *Data Exchange Framework Guiding Principles*[7] for more information on the Guiding Principles for the Data Exchange Framework.

Relevant National Initiatives

The Stakeholder Advisory Group and the Focus Groups identified three national initiatives that might have an impact on the Strategy for Digital Identities. Each is summarized briefly here.

Project US@[8]

Project US@ is an initiative of the Office of the National Coordinator for Health Information Technology (ONC). Its goal is to establish a standard across health care and social services organizations and systems for a uniform representation of consumer addresses.

Studies have indicated there is potential for improved matching through the development and implementation of standards and uniform formats of attributes in digital identities. Through collaboration with standards development organizations and other interested stakeholders, ONC developed and released on January 7, 2022, the initial version of the Project US@ Technical Specification for uniform representation of address.[9]

The Project US@ Technical Workgroup that developed this specification used USPS Publication 28[10] as a foundation due to its widespread adoption in many stakeholder systems. The specification includes formats for United States domestic and military addresses and specifies required and optional address elements and standardized abbreviations.

Use Case: Uniform representation of address for the purposes of improved person matching across health care and social services settings.

Status: Released version 1 of the technical specification for addresses, including physical addresses and mailing addresses that may include a Post Office Box address.

Focus Group members recommended adoption of the specification for the Data Exchange Framework if address is included as an attribute of digital identity.

CARIN Federated Digital Identity[11]

The CARIN Alliance is developing a framework for federating trusted identity assurance at Identity Assurance Level 2 (IAL2). IAL2 represents the level of identity assurance recommended by the National Institute of Standards and Technology (NIST) for remote

---

8 See Project US@ on the HealthIT.gov website for more information about Project US@.

9 Project US@ Technical Workgroup, *Technical Specification for Patient Addresses: Domestic and Military* (Office of the National Coordinator for Health Information Technology, January 7, 2022).

10 *Publication 28: Postal Addressing Standards* (US Postal Service, most recent version June 2020).

11 See Digital Identity on the CARIN Alliance website for more information on the CARIN Alliance's initiative for Federated Digital Identity.

identity proofing for access controls for sensitive information, such as protected health information.[12] The initiative is intended to demonstrate how organizations that ensure the identity of individuals and issue them login credentials (i.e., credential issuers) and organizations that use those credentials to allow individuals to access their data (i.e., relying parties) can collaborate to share certified credentials using a person-centric approach leveraging biometrics and mobile technologies.

Federated trust allows a consumer that has been identity-proofed and issued a digital credential established with one organization to use it to access their data at multiple health care organizations without the need to repeat identity assurance at each one.

Use Case: Consumers accessing and aggregating their health information, and organizations verifying the identity of individuals accessing their information online.

Status: Developed a draft trust agreement among credential issuers and relying parties and conducting a pilot to demonstrate feasibility.

The use case for federated digital identity differs in scope from the Strategy for Digital Identities. CARIN focuses on patient-mediated exchange, and the federated digital identity initiative focuses on an efficient and cost-effective means for assuring identity of patients so they can be granted access to their health information.

This Strategy for Digital Identities is focused on linking records to the correct real person so that providers of health and social services information can access and exchange information with some level of confidence of person identity.

Stakeholder Advisory Group and Focus Group members recommended that CalHHS monitor this initiative and consider incorporating appropriate aspects when pilot testing has demonstrated feasibility and maturity, and when the Data Exchange framework implements individual access.

FAST Reliable Patient ID Management[13]

The FHIR at Scale Taskforce (FAST) was created by ONC and is now housed within HL7, the primary standards development body for the health care industry. FAST identifies Fast Healthcare Interoperability Resources (FHIR®) scalability gaps, defines

---

[12] Paul A. Grassi, Michael E. Garcia, James L. Fento, *NIST Special Publication 800-63-3: Digital Identity Guidelines* (National Institute of Standards and Technology, June 2017).

[13] See the FAST Projects on the HL7 website for more information on the FAST: FHIR at Scale Task Force and the Interoperable Digital Identity and Patient Matching project.

solutions to address current barriers, and identifies needed infrastructure for scalable FHIR solutions.

Use Cases: The FAST Reliable Patient ID Management project is developing three separate paths to enhance patient matching[14] across health care settings:

1. Mediated Patient Matching attempts to match patients through a third-party who is authoritative for patient identity.

   This method uses patient name, date of birth, gender, and address, and optionally insurance ID number or other attributes, to match patients. It is dependent upon an authoritative third-party system, such as a statewide person index, used by all participating organizations.

2. Collaborative Patient Matching leverages unique identifier(s) issued to a patient by organizations that have data about them, such as their health care providers.

   The unique identifier(s) are carried by the patient to each health care setting, and then used by providers at each setting to access information from the organization(s) that issued them. Patient name and date of birth might be included with each unique identifier to provide some assurance of authenticity and protection against identity theft.

3. Distributed Identity Management relies on each health care organization using its own matching algorithms to match a patient against attributes provided by the patient.

   This method is most similar to the use case for the Data Exchange Framework, although it relies on the patient rather than providers for identity attributes. FAST has yet to launch any work against this method.

Focus Group members recommended that CalHHS monitor FAST activities, although still largely in the formative stages as FAST concentrates on other projects.

[14] The FAST Reliable Patient ID Management project uses the term “patient matching” rather than “person matching”. However, most of the concepts should apply to the larger topic of matching persons that may not be patients, for example in a social services context.

Other National Initiatives

Many members of the Focus Groups were participants in the eHealth Exchange[15] and CommonWell Health Alliance[16] national networks, or the Carequality[17] national interoperability framework. Many were also closely following development of the Trusted Exchange Framework and Common Agreement[18] (TEFCA). These members brought their experience with these initiatives and each initiative's use of digital identity to the discussion of the Strategy for Digital Identities.

International Initiatives

In 2016, the Digital ID & Authentication Council of Canada began developing the Pan-Canadian Trust Framework[19] (PCTF). The PCTF comprises a common set of concepts, definitions, processes, conformance criteria, and an assessment approach to establish digital trust among Canadian public and private organizations. The PCTF is intended to promote alignment, interoperability, and confidence of digital identity solutions across organizational, sectoral, and jurisdictional boundaries by complementing existing standards and policies of security, privacy, and service delivery in multiple domains.

The European Union (EU) created the European Digital Identity[20] which is available to EU citizens, residents, and businesses who want to identify themselves or provide confirmation of certain personal information. It is intended for use both online and offline and for both public and private services across the EU as a way of identification or to confirm certain personal attributes for the purpose of access to public and private digital services across the EU. Unlike digital identities in this Strategy, the European Digital Identity is issued to EU citizens primarily as a way for them to identify themselves for services. However, it includes important characteristics meant to establish and preserve privacy and security.

---

15 See the eHealth Exchange website (ehealthexchange.org) for more information about eHealth Exchange national network.

16 See the CommonWell Health Alliance website (commonwellalliance.org) for more information on the CommonWell Health Alliance.

17 See the Carequality website (carequality.org) for more information on the Carequality interoperability framework.

18 See the Trusted Exchange Framework and Common Agreement website on HealthIT.gov for more information about the Trusted Exchange Framework and Common Agreement.

19 See PCTF-CCP | Pan-Canadian Trust Framework Cadre de Confiance Pancanadien (canada-ca.github.io) for more information on the Pan-Canadian Trust Framework.

20 See European Digital Identity | European Commission (europa.eu) for more information on the European Digital Identity.

Strategy for Digital Identities

This Strategy for Digital Identities includes represents the culmination of all recommendations received from Focus Groups, input from the Stakeholder Advisory Group and Data Sharing Agreement Subcommittee, and input from public comment. It includes considerations for both proposed policies and high-level implementation.

Purpose

This Strategy for Digital Identities proposes a single, focused purpose for digital identities for the Data Exchange Framework.

> The purpose and use case proposed for digital identities is to associate accessed or exchanged health and social services information with the correct real person.

Included in this Purpose

This purpose includes two types of activities, both included as purposes for digital identities within the Data Exchange Framework:

Person Matching: Matching a digital identity at one organization to that at another when both are associated with the same real person. This activity is sometimes described as person/patient search or person/patient discovery.

Record Linking: Aggregating or combining health and social services information into a single physical or logical record associated with a single real person. Record linking may take place within an organization, but in the context of the Data Exchange Framework will most often be for information accessed or exchanged across organizational and sector boundaries.

This Strategy proposes that digital identities may be used to associate health and social services information with the correct real person for any of the scenarios anticipated for the Data Exchange Framework, including but not limited to:

- Health care and social services delivery
- Care coordination
- Population health
- Emergency response
- Public health response
- Transitions to and from incarceration

See *Data Exchange Framework Data Exchange Scenarios*[21] for more information on the data exchange scenarios anticipated for the Data Exchange Framework.

Excluded from this Purpose

The purpose of digital identities within the Data Exchange Framework proposed by this Strategy does not include:

- Use of demographic information included as attributes of a digital identity for purposes other than associating health and social services information with a person. The Stakeholder Advisory Group, in its discussion of gaps and opportunities, and the Focus Groups both identified the primary needs for digital identities to be person matching and record linking across organizational and sector boundaries. AB-133 specified that digital identities were to support person indices, the primary purpose of which is to associate health and social services information with the correct real person.

- Development of a "golden record". This Strategy does not propose that the Data Exchange Framework should be intended to establish a single source of truth for all attributes of a digital identity that may be assumed to be 100% accurate. The intent is to define a digital identity that is unique in aggregate, but not establish an authority for the value of any given identity attribute. Establishing a golden record may be a future consideration for digital identities on the Data Exchange Framework.

- A prohibition from exchanging demographics included in the USCDI. Demographic information in the form of attributes of a digital identity serve a different purpose in this Strategy than other information accessed or exchanged using the Data Exchange Framework. All elements of the United States Core Data for Interoperability (USCDI), including data elements in the data group for Patient Demographics, may be accessed or exchanged for any permitted purpose allowable under the Data Sharing Agreement and its associated Policies and Procedures.

  Further, federal regulation and the Data Exchange Framework require exchange of all data elements in the USCDI, including data elements in Patient Demographics. Nothing in this Strategy should be taken as an exception to any requirement by the Data Exchange Framework or federal regulation for organizations to exchange all elements of USCDI that are managed by the entity.

- Using demographics included as attributes of digital identities to stratify populations for analysis purposes. Attributes included in digital identities were selected based on their value in person matching and record linking. This Strategy does not propose

[21] See the *Data Exchange Framework: Data Exchange Scenarios* on CalHHS' Data Exchange Framework website.

that digital identities should be authoritative for the values of demographic attributes. Some demographic data were excluded from attributes of digital identities to preserve individual privacy.

An organization may select or stratify populations using demographic data they already possess. They may also use digital identities for the purpose of linking records and retrieving health or social services information on individuals in populations they identify using the Data Exchange Framework if their purpose for accessing or exchanging information is permitted by the Data Sharing Agreement and its associated Policies and Procedures.

See Permitted Uses of a Statewide Person Index for more information on the permitted uses of digital identities in a statewide person index.

Definition of Digital Identity

The Strategy for Digital Identities proposes specific attributes be included in (and excluded from) digital identities for use on the Data Exchange Framework.

Attributes Included in a Digital Identity

> Digital identities include as attributes selected "Patient Demographics" data elements from the United States Core Data for Interoperability (USCDI) Version 2.

USCDI Version 2. This Strategy proposes the use of Patient Demographics as specified in USCDI v2[22] to align with requirements of the Data Exchange Framework for applicable organizations to exchange elements of the USCDI v2 after October 6, 2022.

Included Attributes. Attributes from USCDI v2 that are proposed by this Strategy as part of digital identities include:

- Name, including family name, given name(s), and middle name or initial
- Other names previously or currently used by the individual
- Date of birth
- Gender (if required by a technical standard or regulation)
- Home and/or mailing address(es)
- Previous address(es)
- Phone number(s)
- Email address(es)

[22] See United States Core Data for Interoperability (USCDI) Version 2 published by the Office of the National Coordinator for Health Information Technology.

These attributes were considered most useful by Focus Group members in person matching and record linking.

Gender is included among attributes of digital identities proposed by this Strategy under limited circumstances. Its inclusion is the result of Focus Group and public input recognizing that many nationally-recognized standards and state regulations require gender as a mandatory attribute in person matching. However, this Strategy strongly discourages its use when not required by an applicable technical specification. Gender has been shown to be of limited discriminatory value in person matching.[23] Historical changes in gender may unintendedly identify transgender individuals, and the code set for gender required in USCDI v2 may not appropriate for all individuals.

The Health Information Technology Advisory Committee (HITAC) that advises the ONC asked the Interoperability Standards Workgroup to evaluate the USCDI Version 3 draft published in January 2022. In its transmittal letter on April 13, 2022, the HITAC recommended "that ONC include in USCDI v3 the Gender Harmony Project's five data elements (gender identity, sex for clinical use, recorded sex or gender, name to use, and pronouns)." [24,25] Future versions of this Strategy may remove gender as an attribute of digital identities or may transition to one or more of the Gender Harmony Project data elements if adopted by ONC in USCDI v3 or later. Until such time as ONC acts on the HITAC recommendation, a statewide person index may not include gender as an attribute in person matching or record linking.

Excluded Attributes. This Strategy proposes to exclude several attributes included as demographics in USCDI v2 from use in digital identities for the Data Exchange Framework:

- Race, ethnicity, or preferred language are not included. Like gender, race and ethnicity have been shown to be a limited discriminatory value in person matching.[23] Some populations may be reluctant to share these demographics, and therefore they are not included for purposes of individual privacy.
- Sexual orientation and gender identity were added to USCDI v2 but are not included as attributes of digital identities. Like race and ethnicity, some populations may be reluctant to share these demographics. Like gender, the

---

23 Eric Heflin, Shan He, Kevin Isbell, et al, *A Framework for Cross-Organizational Patient Identity Management* (The Sequoia Project, 2018).

24 Interoperability Standards Workgroup - U.S. Core Data for Interoperability Draft Version 3 Transmittal Letter (healthit.gov).

25 See The Gender Harmony Project (hl7.org) for more information on the Gender Harmony Project.

code sets for sexual orientation and gender identity required in USCDI v2 may not be appropriate for all individuals. Therefore, both were not included for purposes of privacy and gender equity.

Aliases or other names by which an individual might be known are included as attributes of digital identities if volunteered by the individual or known to the provider. However, this Strategy suggests that organizations should use caution when including previous names so as not to unintentionally identify transgender individuals, especially if including gender as an attribute.

- USCDI version 3 Patient Demographics are not yet included. The value of the additional demographic attributes included in the draft USCDI v3 are not well known. Most systems do not yet implement data elements included in USCDI v3.

As stated earlier, nothing in this Strategy, such as excluding demographic attributes from use in a digital identity, should be taken as an exception to requirements by the Data Exchange Framework or federal regulation for organizations to exchange all elements of USCDI v2 if managed by the entity.

Digital identities include as additional attributes selected identifiers that are uniquely associated with one and only one real person, but only if related to health care services delivery.

Patient demographic attributes are only potentially unique and therefore useful criteria for person matching or record linking in aggregate. Matches may be probabilistic rather than deterministic, and subject to false positives and (perhaps more often in current practice) false negative matching failures. Therefore, there is significant value in including unique identifiers in digital identities as an aid in meeting the “unique digital identity” requirement of AB-133.

Included Attributes. This Strategy proposes to include unique identifiers related exclusively to health systems or health programs in digital identities. Example attributes may be part of digital identities include:

- State or federal identifiers related to health, such as a Medi-Cal or Medicare identification number
- Unique identifiers from other health-related state programs
- Local identifiers related to health systems, such as a health system medical record number or a private payer member identification number

This Strategy proposes that unique identifiers are only to be included as attributes of digital identities if (1) they are unique to a specific individual and (2) they are related to the individual’s health records or health services.

This Strategy recognizes that unique identifiers such as medical record number and health plan member identification number must be accompanied by an unambiguous identification of the organization assigning the identifier. There is no current mechanism to ensure that any such identifier is globally unique, and this Strategy does not propose a method that must be adopted by all participating organizations. Instead, the combination of an identifier unique within an organization and the identity of the organization is globally unique. A statewide person index, discussed later in this Strategy, must develop a method to unambiguously identify each organization participating in the Data Exchange Network in order to associate the organization with its unique local identifier in the index.

Unique identifiers of social services organizations might be included in digital identities as those organizations become participants in the Data Exchange Framework, where and if appropriate.

Excluded Attributes. This Strategy proposes to exclude other unique identifiers from digital identities for the Data Exchange Framework, such as:

- Unique federal identifiers not related to health, such as social security number or passport number
- Unique state identifiers not related to health, such as driver's license number or state ID number

While such unique identifiers may be useful attributes as matching criteria, this Strategy recognizes two primary barriers to including them:

- Some populations may be reluctant to share such identifiers, and they were therefore excluded for privacy purposes
- Collection of these identifiers present a greater target for identity theft, and while all attributes of digital identities, including unique identifiers, will be exchanged securely, these attributes were excluded since unauthorized disclosure was thought to presented too great a potential for consumer harm

Unique identifiers not related to health were excluded as a component of meeting the "secure digital identity" requirement of AB-133.

Table 2 summarizes the attributes that comprise a digital identity for the Data Exchange Framework.

Table 2 Data attributes that define digital identities in the Strategy for Digital Identities for the Data Exchange Framework.

Attribute Source or Category	Attributes
Selected data elements from the US Core Data for Interoperability Version 2	• Name(s) • Date of birth • Gender (limited)[26] • Address[27] • Previous address(es) • Phone number(s) • Email address(es)
Selected identifiers that are uniquely associated with one and only one real person and related to their health records or health services	• State or federal identifiers related to health (e.g., Medi-Cal or Medicare ID) • Local identifiers related to health (e.g., medical record number of plan member identification number)

Standards for Attributes in a Digital Identity

It is well-documented that person matching and record linking can be improved by using standardized content and format for the attributes comprising digital identities.[28] The Strategy for Digital Identities includes consideration for existing technical standards for person demographics and gaps in standards or guidance.

Adopt standard formats and datasets for person demographics specified in United States Core Data for Interoperability (USCDI) Version 2.

This Strategy proposes to use the data attribute names, content, format, and terminology for person demographics established by USCDI v2. [22] USCDI v1 format and terminology standards are widely adopted by health IT systems, and soon will be required for use by certified health IT systems. USCDI v2 format and terminology

---

26 As noted in the text, gender should only be included as an attribute of digital identity when required by a technical exchange standard or state regulation.

27 While USCDI might be interpreted to limit addresses to physical or mailing addresses that include a street number and street, the US@ Project technical specifications include PO Box. The Strategy should adopt the larger definition of the US@ Project and include PO Box addresses that may be especially appropriate for homeless individuals.

28 Audacious Inquiry, *Patient Identification and Matching Final Report* (Office of the National Coordinator for Health Information Technology, February 7, 2014).

standards for most demographic attributes are well-aligned with USCDI v1 and are required for exchange by the Data Exchange Framework after October 6, 2022.

Adopt standard formats and datasets other than USCDI promoted by federal initiatives and identified for use by the Data Exchange Framework.

This Strategy proposes to use nationally-recognized standards, when widely-adopted, as technical standards for attribute names, content, format, and terminology for attributes comprising digital identities. For example, at this time this Strategy proposes the Project US@ *Technical Specification for Patient Addresses*[9] be adopted for the content and format of addresses in digital identities for the Data Exchange Framework.

This Strategy anticipates that Policies and Procedures accompanying the Data Sharing Agreement will identify which nationally-recognized standards are to be used for digital identities. Deliberation on which standards should be included and when should be through a public and transparent function of data governance.

Develop additional required formats and datasets for attributes in digital identities used by the Data Exchange Framework where gaps in nationally-recognized standards exist.

This Strategy recognizes that, despite coordinated national efforts, there remain examples where there is insufficient guidance and/or a gap in technical standards for critical attributes comprising digital identities. For example, there is no widely-adopted standard for the representation of a family name that includes multiple words.

This Strategy proposes that future efforts in digital identities for the Date Exchange Framework should include:

- Harmonizing existing standards where conflicts exist
- Developing standards for content and format where none exists
- Promoting creation of nationally-recognized standards where absent
- Transitioning to recognized standard formats and datasets as federal initiatives mature and nationally-recognized standards emerge and are adopted

Identification of gaps, development of new standards, and transition to nationally-recognized standards should be undertaken through a public and transparent process.

Adoption of existing standards meets a key Guiding Principal of the Data Exchange Framework. Use of standards where they exist and development of guidance to fill gaps both increase linking reliability and are therefore a component of meeting the “unique digital identity” requirement of AB-133.

This Strategy recognizes the need for California to ensure that its own agencies and departments are aligned with the Attributes Included in a Digital Identity and Standards for Attributes in a Digital Identity. This Strategy proposes that the state develop

processes to reconcile its multiple health and social services information collection standards and data dictionaries with this Strategy.

Data Quality

This Strategy recognizes that data standardization alone is insufficient to achieve the goal of accurate person matching and record linking. Organizations have reported that data entry errors (i.e., poor data quality) are the greatest contributor to poor or inaccurate person matching, even greater than errors resulting from terminology-related issues[29] that are the focus of many federal initiatives to improve person matching.

The Stakeholder Advisory Group identified as a gap the need for standardized collection, curation, and use of demographic and social determinants of health data in California. The gap included as an opportunity that the state should establish incentives through public and private payers to improve collection of demographic data. While the target of this gap and opportunity was the exchange of demographic data for purposes other than digital identities, the same efforts would improve data quality for digital identities, person matching, and record linking as well.

Tokenization of Attributes in a Digital Identity

Tokenization, when applied to data security, is the process of substituting a sensitive data element (such as a medical record number or plan member number) with surrogate value known as a "token". The sensitive data elements generally needs to be stored at a centralized location for subsequent reference and requires strong protections.[30,31]

The value of tokenization is that tokens have no extrinsic or exploitable meaning or value. The token is a reference (i.e., a unique identifier) that maps back to the sensitive data through a tokenization system. Critical to the use of tokenization is the existence of a tokenization system available to those using digital identities.

> Consider adopting tokenization of unique identifiers within digital identities to reduce the threat of identity theft.

This Strategy proposes that tokenization be explored as a means to protect digital identities, especially unique identifiers, to mitigate the risk of identity theft.

---

29 *The State of Patient Matching in America* (eHealth Initiative, 2019).

30 Gartner, *Gartner Glossary*.

31 Wikipedia has a further discussion of tokenization that may be useful to the non-technical reader.

In addition to reducing the threat of identity theft, tokenization might be used to mask sensitive data and provide additional consumer privacy. For example, tokens can be used for plan member numbers to avoid reveling consumers that choose self-pay for some or all services. Tokenization might also be used to mask participation in some programs.

Tokenization might also allow the use of unique state and federal identifiers not related to health in digital identities, such as social security numbers or state driver's license numbers, since the primary barrier to these valuable unique identifiers was identity theft.

Tokenization might be an aid in meeting the "secure digital identity" requirement of AB-133. Unfortunately, tokenization requires a component of statewide infrastructure to support the tokenization and referencing process. Tokenization might be a component service of a statewide person index, should one be developed for the Data Exchange Framework. See Statewide Person Index for a discussion of the potential for a statewide person index that might support tokenization.

Statewide Person Index

A common strategy for the attributes and standards for digital identities goes far to improving the effectiveness of person matching and record linking. Many current network and interoperability initiatives rely solely on the ability of network or framework peers to share attributes and agree on a matching person and matching records. Notably, eHealth Exchange, Carequality, the California Trusted Exchange Network, and TEFCA all rely on peer-to-peer person matches and record linking.[32] Standardizing the attributes in a digital identity and data content and format for them, as contained in this Strategy for Digital Identities, should result in better matching performance within California. By adopting national standards, the Strategy for Digital Identities should not conflict with national networks, national frameworks, or federal initiatives.

However, the Focus Groups supported creating a statewide person index to improve the linkage of health and social services information to the correct real person and increase the likelihood of matching an individual served by one organization with their data at another.

Create a statewide person index if funding can be identified and a sustainability plan can be developed.

[32] As a notable exception, the CommonWell Health Alliance includes a network-wide person index and record locator. And while TEFCA is silent on whether a Qualified Health Information Network must have a person index, past and current discussions suggest the potential utility of one.

This Strategy proposes to create a statewide person index to aid in person matching and record linking if funding can be identified and a sustainability plan can be developed.

Included in a Statewide Person Index

This Strategy proposes a purpose of a statewide person index to be to:

- Collect attributes associated with a digital identity from participants of the Data Exchange Framework for use in person matching
- Cross-reference attributes contributed by one organization using the Data Exchange Framework with other organizations

This Strategy proposes that the statewide person index collect all attributes of digital identities, including unique identifiers such as medical record numbers from providers and member identification numbers from health plans. The statewide person index might also expand the attributes to include not only the value, but the provenance of the value(s) as an aid in analyzing data quality, assessing the reliability of attributes, and developing processes for data quality improvement.

Like digital identities, this Strategy proposes that the intent of a statewide person index is not to create a golden record of person demographics. Instead, it is to create an aggregation of the digital identity attributes contributed by organizations using the Data Exchange Framework to facilitate person matching and record linking. It facilitates:

- Identifying and cross-linking all unique identifiers associated with the same real person
- Using a common digital identity across all organizations using the Data Exchange Framework
- Facilitating more complete demographic searches of organizations using the Data Exchange Framework and contributing digital identity attributes to the statewide person index

This Strategy recognizes that a key function of a statewide person index is cross-referencing unique local identifiers associated with a single real person.

This Strategy does not propose a method to validate attributes submitted to the statewide person index by participating organizations. Sustainable methods of validation should be explored in conjunction with sustainability planning. Data provenance may play a key role in understanding data quality of digital identities in a statewide person index, how validation might be accomplished, and opportunities for quality improvement.

While a statewide person index is not a record locator service (often a component of health information exchanges), this Strategy recognizes that the existence of a unique local identifier for a health system, health plan, state agency, or social services organization is a strong indication that health or social services information about that

individual might be housed at that organization and retrievable upon request. As a result, a statewide person index also facilitates:

- Locating the organizations using that Data Exchange Framework that might have health or social services information for an individual

Table 3 summarizes the services that might be provided by a statewide person index.

Table 3 Services provided by a statewide person index in the Strategy for Digital Identities for the Data Exchange Framework.

• Identifying and cross-linking unique identifiers associated with the same real person
• Establishing a common digital identity for organizations using the Data Exchange Framework
• More complete demographic searches of organizations contributing attributes to the index
• Locating the organizations that might have health or social services information for an individual

This Strategy recognizes that a statewide person index is a target for identity theft and will require significant security controls.

This Strategy also acknowledges that successful person matching is not solely a technical solution that can be addressed by a statewide person index. The technical solution must be accompanied by sufficient human resources to analyze and improve the data quality of digital identity attributes, intervene to appropriately merge records where automated technical algorithm results are ambiguous, and tune the technology to best address digital identity attributes in the California population. As a plan for a statewide person index emerges, it will be necessary to determine in detail how the index will be managed, how the data it holds curated and kept current, and how organizations may synchronize with their own person indexes.

Excluded from the Strategy for Person Indices

Not a commitment to create a statewide person index. AB-133 does not require the state to create a statewide person index. The Strategy for Digital Identities is to consider creating a statewide person index if:

- Funding can be identified
- A sustainability plan can be developed

Development of a sustainability plan would include identification of an appropriate organization to implement and operate the statewide person index. Such an organization might be a state agency, a public-benefit organization, or a public-

private partnership. The sustainability plan and identification of the appropriate home for a statewide person index is beyond the scope of this Strategy.

Not a requirement to implement a person index. AB-133 requires digital identities to support person indices. There is no requirement in AB-133 or in this Strategy for public or private organizations using the Data Exchange Framework to implement their own person index.

Not a prescription for local person indices. This Strategy recognizes that many organizations already have a person index. The description of digital identities in Definition of Digital Identity is intended to be a description of how organizations interact with each other to perform person searches and record linking, and not a prescription for the data structure of any local person index. It might, however, guide the data structure and content for a statewide person index.

Not a requirement to use the statewide person index. Organizations would be strongly encouraged, but might not be required, to use the statewide person index. This Strategy acknowledges that increased participation should result in increased effectiveness of a statewide person index. Required participation might be the topic of future public and transparent discussions as the plan for a statewide person index matures. Organizations are also not required to use the statewide person index as a replacement for a local person index already in place.

Not a source of person demographics. The statewide person index is not proposed by this Strategy as a golden record for attributes of digital identities.

The statewide person index would also not be a source for demographic information or contact information to support population health research, for public health outbreak investigation, physician follow-up, or other secondary uses. Those uses would be prohibited under the same terms of the Data Sharing Agreement that prohibit secondary uses of digital identities. See Permitted Uses of a Statewide Person Index for a discussion of permitted purposes.

Potential Uses of a Statewide Person Index

Explore how to involve consumers in managing their digital identities and accessing their health and social services information.

Involving consumers in managing their digital identities. The Data Exchange Framework might explore how to involve consumers to help manage their digital identities. A strategy might be as simple as providing read-only access to their attributes and a means to request corrections to missing or inaccurate data.

This Strategy acknowledges that a requirement for individuals to manage their digital identities as proposed by some FAST use cases may not be realistic and may be overly burdensome. The Data Exchange Framework requires that individuals be

provided access to their health and social services information, which includes information associated with their digital identities. This Strategy recommends that care be exercised in exploring how consumers may be involved in their digital identities, providing the access they desire without imposing burden that may be unrealistic.

Credentialling consumers to access their health and social services information. This Strategy and the definition of digital identities do not include issuing credentials or identity assurance for consumers. However, the services of the organization housing the statewide person index might be expanded to include identity assurance and credentialling in the future as an aid to individual access.

This Strategy acknowledges that the Data Exchange Framework provides for individual access to their health and social services information without a requirement for identity assurance or credentialling of consumers as part of a statewide person index. However, a statewide platform for credentialling and identity assurance might enable future scenarios contemplated for the Data Exchange Framework and be the topic of future public discussion.

Explore the use of tokenization as an expanded service of a statewide person index.

Tokenization was identified by this Strategy as a potential enhancement to privacy and security of digital identities. However, the use of tokens is dependent upon a tokenization system available to those using digital identities. This Strategy recommends that the Data Exchange Framework explore, as part of developing a sustainability plan for a statewide person index, if and when the statewide person index should include tokenization as an expansion to person searches and record linking services.

Related Concepts

A statewide person index is one of a number of potential services that might enhance access and exchange of health and social services information using the Data Exchange Framework. While beyond the scope of this Strategy for Digital Identities, three such services are captured here.

Statewide Consent Registry. Identity is often associated with consumer authorization for providers to access and exchange their health and social services information. Consent to exchange information and management of consumer consent is beyond the scope of this Strategy. However, a shared registry of consumer consent is critically dependent upon and facilitated by a common understanding of reliable person identity. See the Data Sharing Agreement[6] for more information on authorization to access and exchange health and social services information. This Strategy recommends that development of a plan for a statewide person index

consider parallel exploration of a strategy for consent a statewide consent registry or regional consent registries.

Statewide Provider Index. Access to and exchange of health and social services information is facilitated by a common understanding of how to exchange with providers that are using the Data Exchange Framework. A statewide provider directory is beyond the scope of this Strategy. However, discussions with the Stakeholder Advisory Group, Data Sharing Agreement Subcommittee, and Focus Groups identified that a statewide provider directory might be a useful or necessary component of the Data Exchange Framework. A knowledge of provider identity and consumer identity can be combined to facilitate care teams and attribute care responsibilities to appropriate providers.

Statewide Record Locator. A statewide service that registers the location of health and social services information for each consumer, a so-called record locator, is not a component of the Strategy for Digital Identities.

There are several aspects of this Strategy's Definition of Digital Identity, the Attributes Included in a Digital Identity, and the description of a Statewide Person Index that meet some of the objectives of a record locator. As noted earlier, unique local identifiers in a statewide person index coupled with the organization assigning the identifier and cross-referencing of these identifiers to a single digital identity provides strong hints to where health or social services information might exist. Organizations would be able to directly request information from other organizations known by the existence of a local identifier to have records for an individual and use the unique local identifier to reduce the burden of handling and responding to queries and the uncertainty of person matching.

The Data Exchange Framework might, in the future, expand this capability to a full record locator service.

Permitted Uses of a Statewide Person Index

The Data Exchange Framework Guiding Principles to Reinforce Individual Data Privacy and Security, Establish Clear & Transparent Terms and Conditions, and Ensure Accountability created an environment in which the Strategy for Digital Identities, its allowed purposes for use, and its privacy and security requirements needed to balance the safety needs of proper individual identification with the privacy of individuals, weighing privacy most heavily. While not a characteristic of digital identities identified by AB-133, "private digital identities" is a strong component of the Strategy for Digital Identities.

As a result of this strong focus on privacy, this Strategy proposes that the Data Sharing Agreement restrict the use of digital identities accessed through a statewide person index to the intended purpose, namely person matching and record linking. The intent of

this limitation on permitted purpose is to be transparent to consumers regarding the purpose for which demographic information is being collected and used for digital identities.

Limit the use of digital identities in the statewide person index to linking health and social services information to a real person or searching for information in an organization participating in Data Exchange Network exchange.

This Strategy proposes that digital identities that might be made available via a statewide person index may be accessed only by participants of the Data Exchange Framework and signatories to the Data Sharing Agreement. The Data Sharing Agreement and its associated Policies and Procedures should identify the limitations on the permitted purpose for use of digital identities accessed via a statewide person index.

This Strategy proposes that secondary uses of the attributes comprising digital identities accessed via a statewide person index not be permitted. As discussed in Purpose, digital identities are not intended to be a golden record. The intended purpose is solely to link health and social services information to the correct real person. The statewide person index, therefore, should not be used as a repository of demographic data other than for the purposes of person matching and record linking.

Organizations are encouraged to use demographic information already available to them in population health analysis, assessment of equity and access, and other research requiring analysis of person demographics. This limit on the use of a statewide person index in no way prohibits or discourages the access, exchange, or use of demographics using the Data Exchange Framework for any purpose allowed by the Data Sharing Agreement and its associated Policies and Procedures.

Require organizations to follow the same security and privacy requirements for digital identities as those afforded to health information by provisions in the Data Sharing Agreement.

The Data Sharing Agreement and its associated Policies and Procedures explicitly require that organizations afford, at a minimum, the same security, consent, and audit requirements to digital identities for the Data Exchange Framework as the Data Sharing Agreement requires for health information. Some attributes of digital identities may in fact be protected health information with privacy and security requirements under federal law. However, the Data Exchange Framework extends protections to all digital identities and all attributes, whether or not protected health information or protected under other state or federal law.

These requirements are a component of meeting the “secure digital identity” requirement of AB-133.

Additional privacy and security controls on the use of digital identities and the disclosure of personal attributes comprising a digital identity may be included in the Data Sharing Agreement and/or its associated Policies and Procedures.

This Strategy recognizes that the prohibition on secondary uses may increase the burden of organizations with a legitimate need for demographic data for purposes such as analysis of healthcare equity and access or public health investigation. This Strategy also recognizes that while the prohibition of secondary uses may increase consumer trust, it may limit valuable contributions to the public good. There should be continued discussion of permitted uses of information contained in a statewide person index in current and future scenarios contemplated for the Data Exchange Framework through a public and transparent process as the plan for a statewide person index matures.

Security and Privacy

The Focus Group representing the perspective of consumer privacy advocates was asked to consider privacy as a prime charge. However, all Focus Groups discussed security and privacy of digital identities and were asked to weigh the benefits of recommended strategies against the risk to individual privacy. Privacy was a topic of input in discussions with the Stakeholder Advisory Group and Data Sharing Agreement Subcommittee, and a topic of public input.

This Strategy for Digital Identities attempts to strike a balance between protecting individual privacy and ensuring individual safety and effectiveness in person matching and record linking. This Strategy proposes to protect individual privacy in the following ways.

Limited Purpose: The Purpose of digital identities is clearly stated within this Strategy and limited to person matching and record linking.

Limited Attributes: The Attributes Included in a Digital Identity are limited within this Strategy to those useful for the Purpose. Attributes that might be considered of limited value in person matching and record linking are not included in digital identities. Care was taken in discussing the relative value of attributes in person matching and record linking that might be considered sensitive to individuals or populations. Most potentially sensitive attributes were excluded from digital identities. Care was also taken in discussing the relative value of attributes that might also be a target for identity theft. Unique identifiers were limited to those associated with health care delivery.

Requirements of Security and Privacy Safeguards: The Data Sharing Agreement and its associated Policies and Procedures explicitly require that organizations afford, at a minimum, the same security and privacy safeguards to digital identities that are required for health and social services information, including protected health information. While described within this Strategy within the section on Statewide

Person Index, the requirement within the Data Sharing Agreement applies to digital identities in all contexts.

Limited Purpose for Use: The Permitted Uses of a Statewide Person Index is clearly stated within this Strategy as also limited to person matching and record linking. Secondary uses are not to be permitted. The intent of this restriction is to be clear and transparent to individuals on the purpose for which their personal information is being collected in a statewide person index and the purposes for which it may be used. Any expansion in permitted purposes should only be discussed and determined through a public and transparent process.

Implementation of the Strategy for Digital Identities and advancements as the Data Exchange Framework matures must continue to protect individual privacy through privacy and security safeguards.

Potential Burdens and Mitigations

This Strategy for Digital Identities considered the burden for organizations using the Data Exchange Framework to conform to the recommendations herein. Some of the identified burdens and the mitigations applied to them in this Strategy are summarized in Table 4.

Table 4 Potential burdens and mitigations for adopting the Strategy for Digital Identities for the Data Exchange Framework.

Burden	Mitigating Strategy
Existing national standards for patient discovery may not fully support all attributes in the digital identity	• Align with nationally-recognized standards whenever possible • Advocate for new elements in nationally-recognized standards • Provide a runway for organizations to adopt standards for digital identities
Existing electronic health records and other systems may not fully support all attributes of digital identities	• Ensure that there is value in the Strategy to incentivize adoption • Provide a runway for organizations to adopt the attributes of digital identities

Burden	Mitigating Strategy
A statewide person index will require significant funding and effort	• Leverage the substantial investment that health information exchange organizations have made in cross-enterprise person indexes • Leverage the substantial investment providers and state agencies have made in person matching • Investigate opportunities for sustainable funding • Engage stakeholders in continued development and planning • Ensure there is value in the Strategy should a statewide person index not be created • Analyze and quantify the cost savings resulting from improved person matching resulting from a statewide person index • Realize advantages of defining attributes and standards for digital identities until a statewide person index can be created

Key among the mitigating strategies that are part of this Strategy for Digital Identities include:

Align with nationally recognized standards. An attempt has been made throughout this Strategy to identify appropriate national standards, adopt national standards where they exist, develop California standards only when necessary to promote value to the Data Exchange Framework, and advocate for new national standards and migrate to them when adopted.

Ensure value in digital identities. The Strategy is organized in two parts: the Definition of Digital Identity and the strategy for a Statewide Person Index. The value in digital identities alone is enhanced accuracy in person matching and record linking, leading to better association of health and social services information to the correct real person. The statewide person index is an important enhancement to, but not a necessary component of, digital identities.

Leverage existing experience and capabilities. This strategy drew on the substantial expertise and experience of organizations in California in person matching and

record linking. This Strategy acknowledges the substantial investment many organizations, including state agencies, local jurisdictions, provider organizations, health plans, and health information exchange organizations, have made in person matching and record linking. The cost of developing a statewide person index can be lessened and the return on investment maximized by leveraging and integrating with these existing capabilities.[33]

Next Steps

This version of the Strategy for Digital Identities is an initial draft of a Strategy that consolidates recommendations of Focus Groups convened by CalHHS, input from the Stakeholder Advisory Group and Data Sharing Agreement Subcommittee, and input from the public. Next steps for the Strategy include:

1. Conducting a public and transparent process to finalize the attributes of digital identities, nationally-recognized standards to be implemented, and guidance for gaps in standards
2. Advancing and coordinating state participation in digital identities through planning, alignment of state requirements and the Data Exchange Framework, and coordination with/of state initiative impacting or impacted by digital identities
3. Revising the Policies and Procedures of the Data Sharing Agreement to include the attributes of digital identities and the standards to be implemented
4. Exploring funding and sustainability to create a statewide person index

[33] See *A Framework for Cross-Organizational Patient Identity Management* referenced earlier for a discussion of cost savings that might be realized from improved person matching.