California Health & Human Services
Data Exchange Framework

Strategy for Digital Identities

Table of Contents

Introduction and Background 1
AB-133 Requirement for a Strategy for Digital Identities 1
Gap Identified by the Stakeholder Advisory Group 1
Definitions for Strategy for Digital Identities 2
Process for Developing a Strategy for Digital Identities 4
Development Process 4
Application of Guiding Principles 6
Relevant National Initiatives 7
Strategy for Digital Identities 11
Purpose 11
Definition of Digital Identity 12
Permitted Uses 17
Statewide Person Index 19
Potential Burdens and Mitigations 23
Next Steps 24
Summary 24

Table of Tables

Table 1 Application of Guiding Principles for the Data Exchange Framework to the development of the Strategy for Digital Identities 6
Table 2 Data attributes that define digital identities in the Strategy for Digital Identities for the Data Exchange Framework. 15
Table 3 Services provided by a statewide person index in the Strategy for Digital Identities for the Data Exchange Framework. 20
Table 4 Potential burdens and mitigations for adopting the Strategy for Digital Identities for the Data Exchange Framework. 23

Table 5 Summary of the requirements and considerations for the Strategy for Digital Identities for the Data Exchange Framework. 24

Table 6 Summary of the Strategy for Digital Identities for the Data Exchange Framework. 25

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 the 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, permitted purposes for using digital identities, and the role of person indices.

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 coordinated person identity matching services are needed to improve effective exchange of health and social services information.

Effective exchange and use of health care 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 resolution and record-linking technologies within their organizations. However, the Stakeholder Advisory Group noted that there is no systematic coordination of digital identities, person resolution, or record linking across organizational boundaries in California, limiting the efficacy of cross-organizational data exchange. As a result, organizations may:

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

- Fail to locate existing health or human service 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 human 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 resolution, 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.

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 Strategy for Digital Identities

The following definitions were adopted 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.

[2] Add link to DxF Gaps and Opportunities document.

Digital Identity is 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 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, gender, address, and phone number).

Secure Digital Identity is 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 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 a digital identity that is collected, used, and shared only in allowed ways for allowed purposes with trusted individuals to protect personal privacy.

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 patient 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 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
- Human service organizations
- California state agencies and departments

The membership of each Focus Group drew most heavily from California stakeholders. However, organizations outside of California were represented as well to ensure the

[3] Rosters for each Focus Group can be found on CalHHS’ Data Exchange Framework website.

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.

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 in a digital identity
- Permitted use of digital identities and limitations on secondary use to protect privacy
- The role of person indices and a potential statewide index
- Barriers to adoption of a California 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]

[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] Add link to Data Exchange Framework documents.

[6] Add link to DxF Data Sharing Agreement and Policies and Procedures documents.

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 summaries considerations and design activities for each of the Guiding Principals 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 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

[7] Add link to DxF Guiding Principles document.

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 summaries 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

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

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.

Stakeholder Advisory Group and 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 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

[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.

[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).

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 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 across health care settings:

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

[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.

   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.

Other Initiatives

Many members of the Focus Groups were participants in the eHealth Exchange[14] and CommonWell Health Alliance[15] national networks, or the Carequality[16] national interoperability framework. Many were also following closely development of the Trusted Exchange Framework and Common Agreement[17] (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.

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

[15] See the CommonWell Health Alliance website (commonwellalliance.org) for more information on the CommonWell Health Alliance.

[16] See the Carequality website (carequality.org) for more information on the Carequality interoperability framework.

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

Strategy for Digital Identities

Purpose

The purpose and use case 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 may go by other names, including “patient matching”, “person resolution”, or “record linking”, all of which are intended to be included in the purpose for digital identities within the Data Exchange Framework.

This purpose may include the aggregation of health and social services information accessed or exchanged across organizational and sector boundaries into a single physical or logical record associated with the real person.

Digital identities may be used to associate health and human services information with the correct real person for any of the scenarios anticipated for the Data Exchange Framework, including but not limited to:

- Care coordination
- Population health
- Emergency response
- Public health response
- Transitions from incarceration

See *Data Exchange Framework Data Exchange Scenarios*[18] 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 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 need for digital identities to be patient 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.

[18] Add link to DxF Data Exchange Scenarios document.

Development of a "golden record". The Data Exchange Framework is not 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 than 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 if for permitted purposes allowable under the Data Sharing Agreement and its associated Policies and Procedures.

Using demographics included as attributes of digital identities to stratify populations for analysis purposes. Attributes included in digital identities were selected on the basis of their value in person matching and record linking. Digital identities are not authoritative for the values of demographic attributes. Some demographic data were excluded from attributes of digital identities to preserve individual privacy.

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 is their purpose for accessing or exchanging information is permitted by the Data Sharing Agreement and its associated Policies and Procedures.

See Permitted Uses for more information on the permitted uses of digital identities.

Definition of Digital Identity

Attributes Included in a Digital Identity

Digital identities include selected “Patient Demographics” attributes from the United States Core Data for Interoperability (USCDI) Version 1.[19]

Included Attributes. Attributes from USCDI v1 that are part of digital identities include:

- Name, including family name, given name(s), and middle name or initial
- Date of birth

[19] See United States Core Data for Interoperability (USCDI) Version 1 published by the Office of the National Coordinator for Health Information Technology.

- Address
- Previous address(es)
- Phone number(s)
- Email address(es)

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

Excluded Attributes. Several attributes included as demographics in USCDI v1 are not included in digital identities:

- Race, ethnicity, or preferred language are not included. These attributes are not consistently reported by individuals (e.g., reported values may depend on context) and are therefore not reliable as matching criteria. Some populations may be reluctant to share these demographics, and therefore they are not included for purposes of individual privacy.
- Previous name and gender are not included. Gender is of limited value as a matching criterion. Previous name and/or gender may also unintendedly identify transgender individuals, and the code sets for gender supported in USCDI v1 are not 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 not excluded as attributes of digital identities if volunteered by the individual or known to the provider. However, digital identities are not to specifically identify previous names.
- USCDI version 2 or version 3 demographics are not yet included. The value of the additional demographic attributes included in USCDI v2 and the draft USCDI v3 are net well know. Most systems do not yet implement USCDI beyond version 1.

Digital identities include as additional attributes selected identifiers that are uniquely associated with one and only one real person.

Patient demographic attributes are generally only useful criteria for person matching or record linking and potentially unique 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. Unique identifiers related exclusively to health systems or health programs. 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

Unique identifiers are only 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.

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

Excluded Attributes. Other unique identifiers are not included in digital identities, 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, there are 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 security and they 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 1	• Name(s) • Date of birth • Address • 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 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. 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 1.[19]

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.

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

Nationally-recognized standards, when widely-adopted, should also be included as technical standards for content and format for attributes comprising digital identities. For example, the Project US@ *Technical Specification for Patient Addresses*[9] should be adopted for the content and format of addresses in digital identities for the Data Exchange Framework.

It is anticipated 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 a through a public and transparent function of data governance.

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

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.

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 a through a public and transparent function of data governance.

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.

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 a non-sensitive equivalent. This substitute is referred to as a “token”.[20]

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.

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

[20] Wikipedia has a further discussion of tokenization, from which this description was taken.

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, 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.

Permitted Uses

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, the Strategy for Digital Identities restricts the use of digital identities using the Data Exchange Framework. The intent of this limitation on permitted purpose is also 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 Data Sharing Agreement to linking health and social services information to a real person or searching for information in an organization participating in Data Exchange Network exchange.

Digital identities are made available only to 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.

Secondary uses of the attributes comprising digital identities are not 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. There is no expectation or guarantee of the accuracy of demographic information in digital identities greater than in an organization's own systems.

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. However, this limit on the use of digital identities 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. Demographic attributes that could be gleaned from digital identities must be requested from Data Exchange Framework participants subject to permitted purposes.

Require organizations to follow the same security, consent, minimum necessary, and audit 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.

The Data Sharing Agreement should also limit the disclosure of digital identity attributes to the minimum necessary to meet the intended purpose, which is the linking of health or social services information to the correct real person. In particular:

- Sharing of demographic attributes other than unique identifiers not already known to the organization as part of a person search or record linking is not allowed
- Sharing of local identifiers is allowed only for permitted purposes under the Data Sharing Agreement

This again in no way prohibits or discourages the access, exchange, or use of demographic attributes unknown to an organization using the Data Exchange Framework. Demographic attributes that could be gleaned from digital identities must be requested from Data Exchange Framework participants subject to permitted purposes.

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.

Statewide Person Index

A common strategy for the attributes and standards for digital identities goes far to improving the effectiveness of person searches and record linking. Many current network and interoperability initiatives rely solely on the ability of network or framework piers to share attributes and agree on a matching patient and matching records. Notably, eHealth Exchange, Carequality, the California Trusted Exchange Network, and TEFCA all rely on pier-to-pier person matches and record linking.[21] 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 human services information to the correct real person and increase the likelihood of matching an individual served by one organization with their data at another.

> Explore creating a statewide person index if funding can be identified and a sustainability plan can be developed.

Included in a Statewide Person Index

The purpose of a statewide person index would 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

Like digital identities, 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 patient 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

[21] 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.

- Facilitating more complete demographic searches of organizations using the Data Exchange Framework and contributing digital identity attributes to the statewide person index

While a statewide person index is not a record locator service (often a component of health information exchanges), the existence of a unique local identifier for a health system, health plan, state agency, or social service 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.

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 explore the creation of 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 not required, to use the statewide person index as increased participation should result in increased effectiveness. 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 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.

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.

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

This Strategy for Digital Identities acknowledges that the Data Exchange Framework may provide individual access to their health and social services information. Individual access might in turn require identity assurance and credentialling of individuals, including persons with digital identities in a statewide person index.

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

Tokenization was identified 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. The Data Exchange Framework should 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 capture 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.

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. As noted earlier, unique local identifiers in a statewide person index provides strong hints to where health or social services information might exist. The Data Exchange Framework might, in the future, expand this capability to a full record locator service.

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 summaries in Table 4.

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

Burden	Mitigating Strategy
Easting 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
A statewide person index will require significant funding and effort	• 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 • 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 migration 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 enhancement, but not a necessary component, to digital identities.

Next Steps

This version of the Strategy for Digital Identities was created to support public comment. Next steps for the Strategy include:

1. Refining the Strategy for Digital Identities through the public comment process
2. Ensuring the privacy and security provisions for digital identities contained within the Strategy for Digital Identities are incorporated in the Data Sharing Agreement and its associated Policies and Procedures
3. Publishing the initial version of the Strategy for Digital Identities by July 31, 2022, as required by AB-133
4. Creating a data governance process to finalize the attributes of digital identities, nationally-recognized standards to be implemented, and guidance for gaps in standards
5. Revising the Policies and Procedures of the Data Sharing Agreement to include the attributes of digital identities and the standards to be implemented
6. Exploring funding and sustainability to create a statewide person index

Summary

The following Table 5 summaries the primary factors that influenced the Strategy for Digital Identities.

Table 5 Summary of the requirements and considerations for the Strategy for Digital Identities for the Data Exchange Framework.

1. Meet 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. Adopt consumer privacy as a key component of the Strategy, in additional to security as identified in AB-133.

3. Address 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. Engage stakeholders through consultation with the Stakeholder Advisory Group; convening Focus Groups to capture diverse stakeholder perspectives of over fifty strategic, technical, and operational experts inside and outside of California; and discussions with the Data Sharing Agreement Subcommittee.
5. Apply the Guiding Principles developed for the Data Exchange Framework in consultation with the Stakeholder Advisory Group. Table 1 summaries how Guiding Principles were considered in the Strategy.
6. Draw on the experience and success of health information exchange and interoperability already present in California.
7. Consider the progress of national initiatives, state health information exchange, national networks, and national interoperability frameworks.

The following Table 6 lists in one place the strategies that are outlined in this document

Table 6 Summary of the Strategy for Digital Identities for the Data Exchange Framework.

Digital Identities

1. The purpose and use case for digital identities is to associate accessed or exchanged health and social services information with the correct real person.
2. Digital identities include selected “Patient Demographics” attributes from the United States Core Data for Interoperability (USCDI) Version 1. Those selected attributes are listed in Table 2.
3. Digital identities include as additional attributes selected identifiers that are uniquely associated with one and only one real person. Those selected attributes are also listed in Table 2.
4. Adopt standard formats and datasets for person demographics specified in United States Core Data for Interoperability (USCDI) Version 1.
5. Adopt standard formats and datasets other than USCDI promoted by federal initiatives and identified for use by the Data Exchange Framework.
6. Develop additional required formats and datasets for use by the Data Exchange Framework where gaps in nationally-recognized standards exist.
7. Consider adopting tokenization of unique identifiers within digital identities to reduce the threat of identity theft.
8. Limit the use of digital identities in the Data Sharing Agreement to linking health and social services information to a real person or searching for information in an organization participating in Data Exchange Network exchange.

9. Require organizations to follow the same security, consent, minimum necessary, and audit requirements for digital identities as those afforded to health information by provisions in the Data Sharing Agreement.
10. Explore the use of tokenization as an expanded service of a statewide person index.

Statewide Person Index

11. Explore creating a statewide person index if funding can be identified and a sustainability plan can be developed. Services that might be provided by a statewide person index are listed in Table 3.
12. Explore how to involve consumers in managing their digital identities and accessing their health and social services information.
13. Explore the use of tokenization as an expanded service of a statewide person index.