Health Digital Identity
Update 2019
Background
What is a Health Digital Identity

The electronic representation and description of an entity in the digital world of health
What is a Health Digital Identity

It is a collection of many different pieces of information (attributes) about an entity in a digital format that have been creditably verified.

Depending on the type of transaction, the attributes needed from the entity to complete that transaction could be different.
Health Digital Identity ecosystem – Objectives

- Participants can be sure that other parties they are transacting with are who they claim they are.
- Participants feel safer sharing their information with other participants in the ecosystem, and they have control over what they share.
- Digital identity services are cost effective and easy to use.
- Participants can trust that others participating in the ecosystem are following the system rules and that they accept the obligations of their designated role.
- The digital identity solution is secure, resilient and interoperable.
Health Digital Identity: The benefits

- Patient and clinical safety
- Improve information privacy and confidentiality
- Improve user experience
- Cost savings
Scope: Current = People

Tangata whaiora/persoons seeking health: consumers/patients

Healthcare contributors: practitioners or providers
Scope - Future

Healthcare organisations and facilities

Things: IT applications and devices

Consent and delegation
Equity Principles

- Support access to healthcare in New Zealand
- Be responsive to issues of equity and accessibility
- Give due recognition to the Treaty of Waitangi
- Accept that the attributes of personal identity can evolve over time
- Comply with New Zealand legislation, regulation and social licence
- Provide an exemplary digital identity-based authentication service
- Comply with Standards
- Channel agnostic
The journey so far

- Technical working group, technical, clinical, central government
- Alignment with whole of government
- International trends
- Contextualisation to healthcare
- Legal advice
- Implementation
Considerations

- Stages of life, capacity and legal state of individuals
- Relationships: Family/whanau and caregivers
- Non-registered health professionals
- Verification processes
- Binding process
- IAM
- Social expectations, policy, legislation
Architecture
A person is required to prove their identity many times in their life journey – current scenario
How we can prove who we say we are using Health Digital Identity?

Lucy is 18 and wants to:
- enrol at university
- open a bank account
- prove she is vaccinated for her OE.

1. Accredited through the Trust Framework

INFORMATION PROVIDERS

Giving consent through a personal information app lets Lucy fully control and have a record of which information is used for which service.

2.

3. Having control over her information in one place means Lucy can use it to shorten processes, save time, make other services easier.

SERVICES

- Show that you’re vaccinated
- Enrol at university
- Open a student bank account
Our development approach

Solution development

• Phase 1 – proof of concept
  • Proposed ecosystem model can deliver the objectives
  • Technology is available and scalable
  • Supplier and consumers will participate
  • Cost effective to the sector
  • Organisations can adopt in a modular manner

• Phase 2 – confirm design of solution model and develop implementation roadmap
• Phase 3 – development and implementation of solution

Framework development

• Health Digital Identity Trust Framework
  • Rules and governance
  • Relationship with our current health identifier

• Health Digital Identity Standards Framework and relevant standards
Health Digital Identity – Implementation

**Users**
Entities for which the system provides digital identity, for the purpose of allowing them to engage in transactions.

**Identity Providers (IPs)**
Entities that hold user identity attributes, attest to their veracity and complete identity transactions on behalf of users.

**Attribute exchange platform**
Enables and completes transactions by matching identity queries from relying parties with attributes from the identity providers and exchanging attributes of proof of identity.

**Relying Parties (RPs)**
Entities that accept attestations from identity providers about user identity to allow users to access their services.

**Governance body**
Entity that oversees the smooth operation and evolvement of the identity system and makes the rules, such as the development and maintenance of the Health Digital Identity Trust framework.
Why can’t we just use the NHI and HPI?

Health Digital Identity and Health Identifiers are used for different purposes.

Health Identifiers are used to uniquely identify health events that happen to an entity or are performed by an entity in the health ecosystem whether digitally or not, without revealing the entity’s identity unless necessary.

Health Digital Identity is used by entities participating in a health digital transaction to prove who they say they are to the other parties collaborating in the same transaction.

It is possible that a Health Digital Identity may be linked to multiple Health identifiers.
Wouldn’t it be easier to have a NZ Social Security Number?

Yes

However we legislated against this is 1993
What is the difference between Digital authentication and digital identification

Digital authentication is designed to answer the question ‘Is that you?’
- Digital solutions using information they have to establish that the person accessing my account or device is me (e.g. a PIN, password, biometric identifier or other form factor)

Digital identification is intended to answer the question ‘Who are you?’
- Using a recognised trusted party to digitally prove I am the person I said I am
Dr. Hogg registered with MoH to obtain a Health Digital Identity credential

1. Dr. Hogg request MoH to issue him a DI credential containing the attributes he provided

2a. Request to verify Passport details

2b. Passport details verified

3a. Request to verify CPN, RA# and Scope of practice

3b. Attributes verified

4. Issue credential

DHB give Dr. Hogg access to their IT Applications based on his scope of practice

1. Provide credential and/or attributes

2. Dr. Hogg’s credentials and/or attributes

3. Request verification of Dr. Hogg’s credential and attributes

4. Assertion

5. DHB establish Dr. Hogg’s access rights and time limit

6. Confirm access rights granted

7. Inform Dr. Hogg’s access rights

8. Log into DHB Application using DI credential

These steps are optional once Dr. Hogg is established in the DHB’s IAM

MoH (Identity provider)

Identity Information Verification service

HPI

DHB IAM

Provider portal

DHB Admin Applications

DHB Clinical Applications

20
Health Digital Identity – presentation options

Health Digital Identity could be stored in the form of a “Digital wallet”

Health Digital Identity could be implemented in the form of:

- A chip
- A QR code
- A bar code
- A mobile app
Where we are at today
Health Digital Identity - Summary Progress

Standards
- Health Digital Identity Standards Assurance Framework first draft completed
- Health Digital Identity Data Composition Standard started

Supporting policy and guidelines
- Health Digital Identity Trust Framework first draft to be completed March 2020

Proof-of-Concept
- Users cases identified investigating technology options