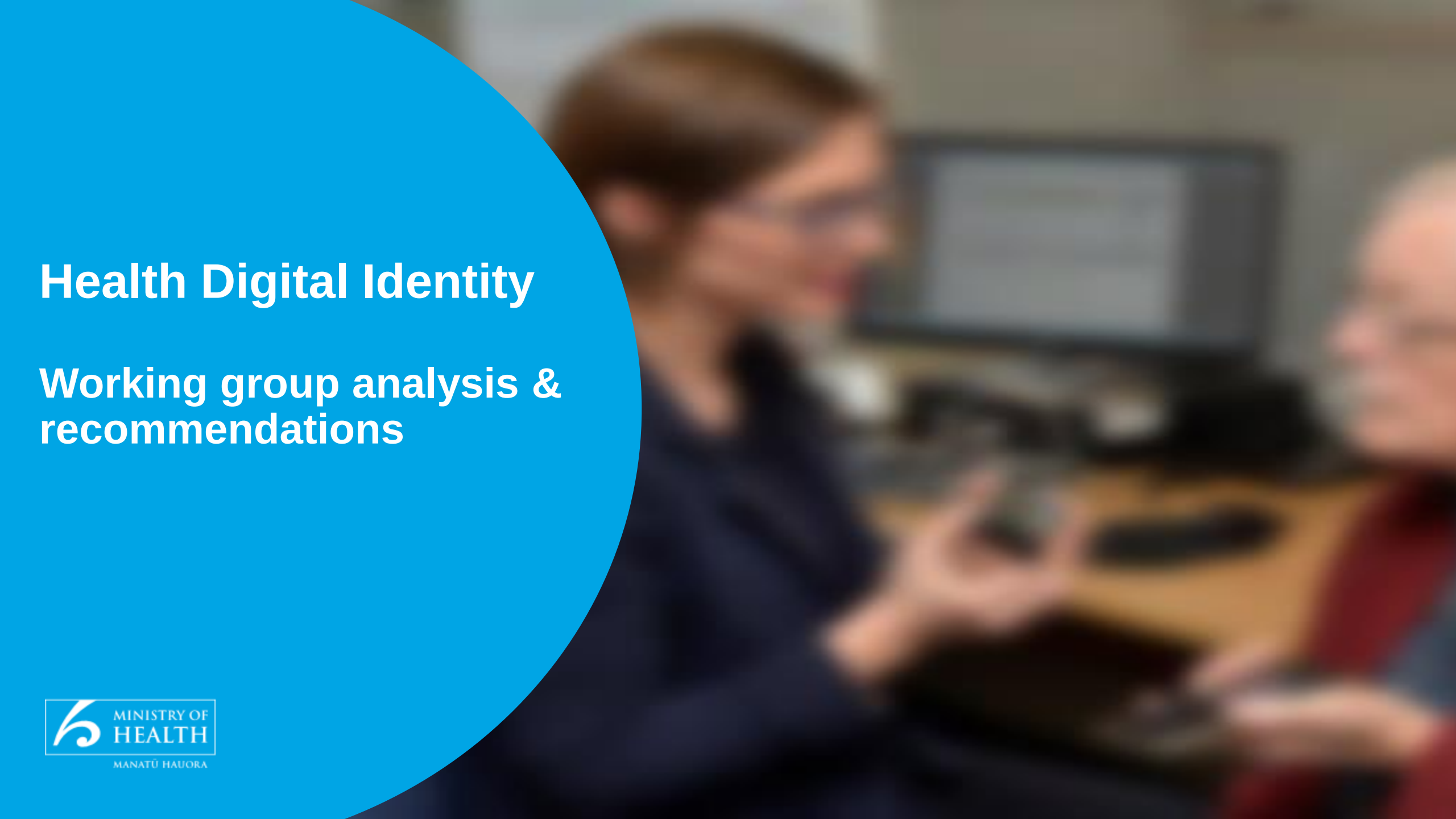
Health Digital Identity

Working group analysis & recommendations



MINISTRY OF HEALTH
MANATŪ HAUORA

Definition of Health Digital Identity

- Cambridge Dictionary:

  Identity is "who a person is, or the qualities of a person or group that makes them different from others".

- yourdictionary.com

  The definition of identity is who you are, the way you think about yourself, the way you are viewed by the world and the characteristics that define you.

Extending the above to the digital world…..

Digital identity is the electronic representation and description of an entity in the digital world of health.

Characteristics of Health Digital Identity and Digital Identity System

- Health Digital Identity is a collection of many different pieces of information (also known as attributes) about an entity in a digital format, which the entity can control and use to complete digital health transactions.
- Attributes of a health digital identity help parties collaborating in a digital health transaction to ensure the other parties they are dealing with are who they said they are.
- To securely transact in a digital world, every party involved in a digital health transaction must have a health digital identity. This includes people, other legal entities (such as organisations) or assets (such as IT applications or medical devices).
- Levels of trust and confidence about a digital identity (i.e. level of assurance) to other parties participating in a digital transaction, are determined by the attributes presented and their source based on a trust framework.
- Proof of identity can be communicated between entities in a standardised digital format; and can be easily aggregated as required for a transaction.

Characteristics of Health Digital Identity and Digital Identity System (continued)

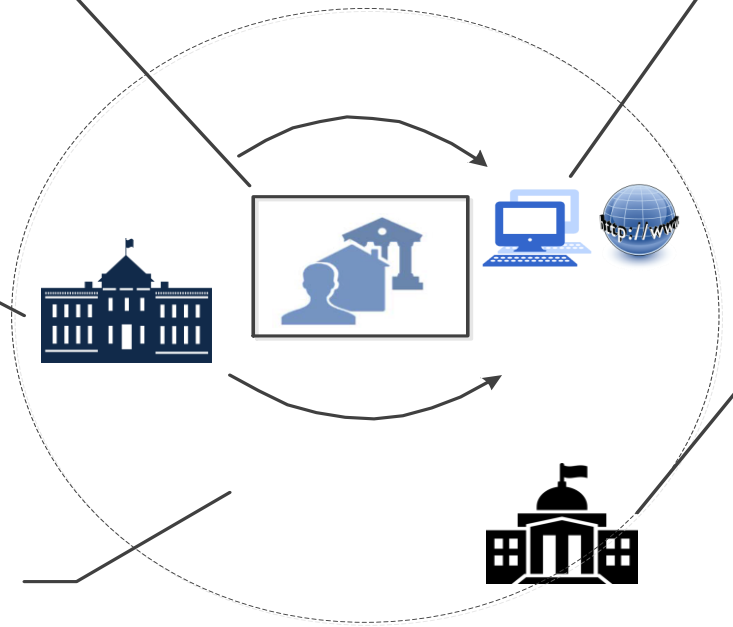
- Anyone who uses other peoples' digital identity to conduct an unauthorised business transaction commits an illegal act i.e. commits identity fraud
- Individuals who act on behalf of another person to conduct business would carry out such duties using their own digital identity, and must have either:
  - Explicit delegation from the person they are acting for, e.g. Power of Attorney; or
  - Implicit delegation as governed by legislation or policy, e.g. delegation of a digital identity to a guardian
- Health Digital Identity "systems" should be designed to adapt to the continuous evolution of identity requirements of different transactions. For example, different attributes will be required when a person is logging into a patient portal vs collecting a script from a pharmacy.

Relationships between Health Digital Identity and existing Health Identifiers e.g. NHI numbers

- Health Digital Identity and Health Identifiers are used for different purposes:
  - Health Identifiers are used to uniquely identify health events/activities 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.
- Depending on the context, it is possible that a Health Digital Identity may be linked to multiple Health identifiers.

Recommended Health Digital Identity solution model

- The recommended model is a federated model that will operate ~~on a basic shared structure based~~ on a trust framework consisting of the following roles and functions:



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

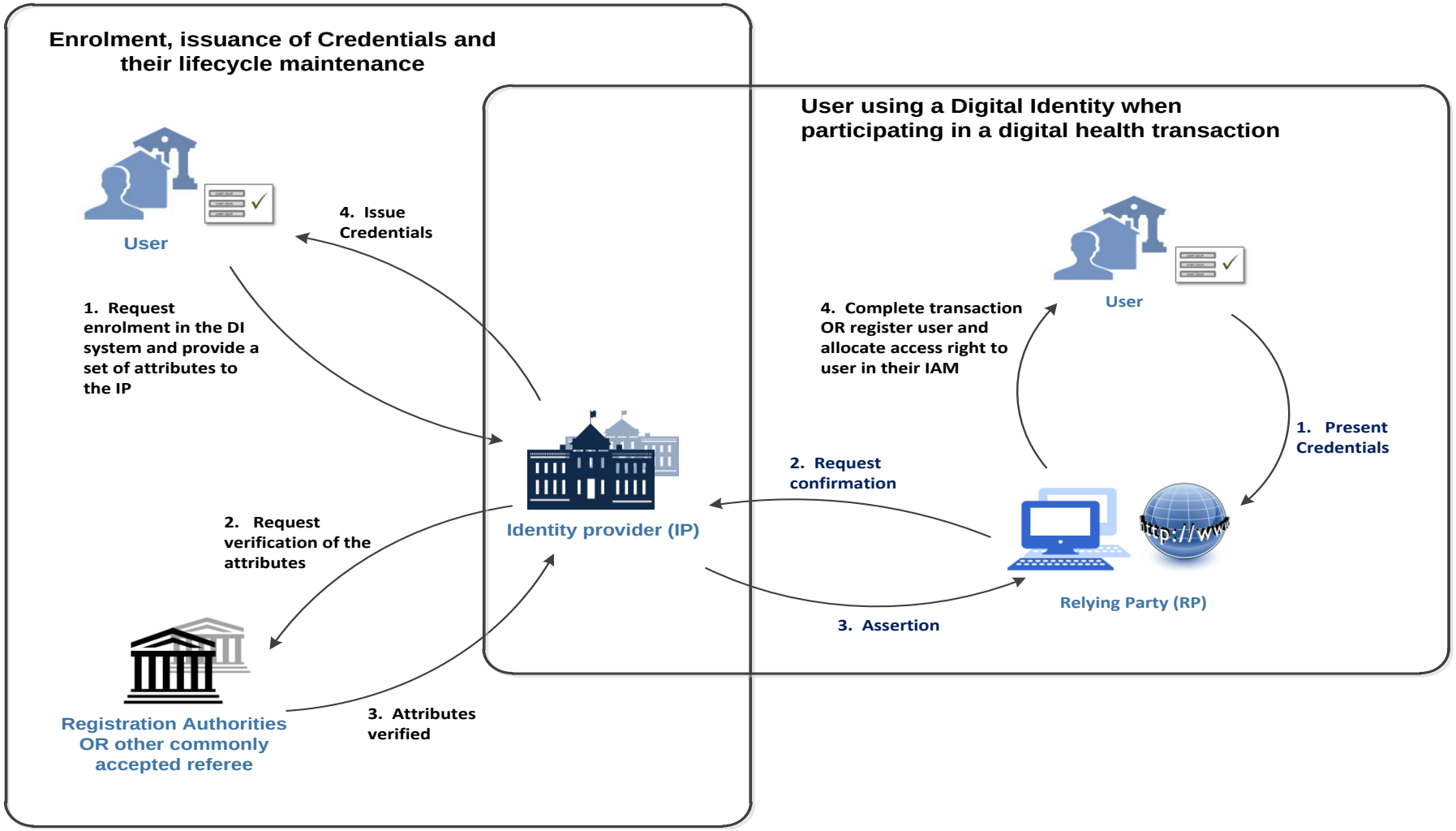
Relying Parties (RPs)
Entities that accept attestations from identity providers about user identity to allow users to access their services

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

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.

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

Recommended Health Digital Identity solution model – How it works



High Level Roadmap (Proposed)

Subject area of development	2018/2019	2019/2020	2020/2021	2021/2022
Supporting Standards				
Consumer Health Identity Standard – HISO 10046	Well adopted at present; will be reviewed in relation to DI requirement	Changes published and adoption continued	Changes adopted by most of the sector	Changes fully adopted by the sector – ongoing update and monitoring of standard adoption and application
Health Provider Index Standard (clinicians, organisations, facility only) – HISO 10045.	Public consultation of changes in relation to DI requirement. (This standard is currently in development.)	Changes published and adoption commenced	Adopted by most of the sector	Changes fully adopted by the sector – ongoing update and monitoring of standard adoption and application
Systems and Devices Naming Standard – HISO 10049 **(To be led by Interoperability TWG - may include aspects of/from the HPI, HISF, - other agencies doing similar things e.g. Education)**	Review existing standards in relation to Digital Identity	Standard development including public consultation	Adopted by most of the sector	Changes fully adopted by the sector – ongoing update and monitoring of standard adoption and application
Health Information Security Framework – HISO 10029	Well adopted at present; will be reviewed in relation to DI and other requirements	Changes published and adoption commenced	Changes adopted by most of the sector	Changes fully adopted by the sector – ongoing update and monitoring of standard adoption and application
Health Digital Identity Attribute Data Standards	Initial scoping and Development	Public consultation	Published and adoption commenced	Standard fully adopted by the sector – ongoing update and monitoring of standard application
Health Digital Identity Assurance Framework	Initial scoping.	Standard development including public consultation	Published and adoption commenced	Standard fully adopted by the sector – ongoing update and monitoring of standard application
Health Information Governance Guideline in relation to DI – HISO 10064	Limited adoption at present; will be reviewed in relation to DI and other requirement	Changes published and adoption commenced	Changes adopted by most of the sector	Standard fully adopted by the sector – ongoing update and monitoring of standard application
Supporting Policies and Guidelines				
Health Digital Identity Trust Framework (covering Consent, delegations, information sharing, monitoring, etc.)	Initial scoping	Development and Public consultation	Published and adoption commenced	Guideline adopted by the sector – ongoing update and monitoring of application
Business rules to link Health Identifiers to Digital Identities going beyond what we are doing today for NHI and HPI	Initial scoping	Development and Public consultation	Published and adoption commenced	Guideline adopted by the sector – ongoing update and monitoring of application
Solution development and rollout				
Solution approach confirmed	Proof of concept to establish technology options	Solution options confirmed, and business case to proceed with solution selection approved.		
Solution development		Solution selected and business case approved.	Development completed, pilot rollout started	Pilot completed
Solution rollout				Rollout to early adopters

Challenges

- **Impact is extensive** The implementation will impact all consumers and providers of health services, as well as other organisations whose business relies on accurate health information/statistics; therefore rollout has to be carefully planned to ensure minimum disruption to service provision.
- **Uptake of the solution** This depends very much on social acceptance that the solution is secure and can be trusted to protect users' information from uses other than as authorised by the users. This is the ***biggest challenge*** to the rollout of Health Digital Identity.
- **Vendor capability to deliver and support a viable solution** Whether there are vendors from the market who can deliver and support the solution model proposed that is ***affordable*** to the sector.
- **Dependencies** Availability of standards and policies required to support the implementation of Health Digital Identity (refer roadmap).

Next Step

- Develop high level plan and Terms of Reference for the following key activities in each of the three work streams:
  - Development of Health Digital Identity Attribute Data Standard and Health Digital Identity Assurance Framework
  - Development of Health Digital Identity Trust Framework (covering Consent, delegations, information sharing, monitoring, etc.)
  - Identify and engage with solutions vendors who can assist us to work on a proof of concept to establish technology options