Connecting Health

The Challenge

The current Connected Health network is in essence a closed, multi-provider wide area network. It does allow for inter provider collaboration with a degree of communication safety due to its private architecture, yet at the same time it stands isolated from consumer access and modern internet based technologies.

The Objectives

- Develop a Connected Health 2.0 framework that will support and enable health providers to safely share health information across networks between themselves and to health information consumers.
- Develop a Connected Health 2.0 framework that will allow system developers to take full advantage of what emerging technologies have to offer.
- To augment the existing Connected Health network such that it loses none of its' value or benefit yet so that it also does not eventually become an isolated artefact.

The Principles

Agnostic: connectivity can be provided over a range of network types and network providers. The choice of which network and network supplier should be made by provider of the service/application.

Trust: data transmitted between services and applications is safe and private, and delivery is assured. Trust should be provided from the services and applications, as opposed to relying on networks.

Fit for purpose: a standard reference model will be available, applied, and assured to ensure that connectivity constructs are appropriate and consistent.

Low cost of entry: connectivity will be supported over a range of network types so that application providers can choose the best connectivity method to suit health use cases and the reference model. The Internet should be considered first.

Open: by default, connectivity should allow any provider to provide health applications and services without connectivity being a constraint.

Dependencies

In order to move from a network centric approach to supporting health outcomes by connecting health, a number of dependencies need to be addressed that are typically outside a traditional network view.
These include:

- standards for application and information providers, to ensure that over time applications are not dependent on networks to meet their security and use case requirements.
- Communication and education for health providers and entities, to ensure a consistent approach and that the roadmap is implemented.

Graduated Trust Model – Associated Risk

Controls are applied appropriately relative to the degree of risk associated to a breach of inappropriate data access or use. An application risk assessment is a recommended course of action prior to publishing a service for the health sector onto the internet.

LOW

No risk of privacy breach or illegitimate transaction. Dataset does not contain identifiable patient information and does not relate to commercial transactions

MEDIUM

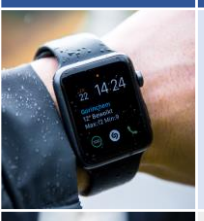
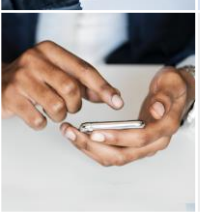
Risk of individual privacy breach or illegitimate transaction

HIGH

Risk of privacy breach for many individuals
Risk of many illegitimate transactions or falsified records

VERY HIGH

Risk of privacy breach for many individuals
Risk of many illegitimate transactions or falsified records
Risk of fraud
Risk of illegal drug access

	Health Information Access Scenarios	LOW	MEDIUM	HIGH	VERY HIGH
	**Wearables / Telemetry** Examples might be Smart watches or blood pressure monitors. Telemetry devices typically measure and transmit monitoring information.	Encryption only TLS	Encryption Authentication	Encryption Authentication Audit	Encryption Authentication Device filtering Audit Access expiry PKI
	**Patient / Consumer** Patient portals or other kinds of online patient services. Services available to the public. Dataset accessed is likely to be personal.	Encryption only TLS	Encryption Authentication	Encryption Authentication Captcha Audit	Encryption Multi Factor Authentication Audit Access expiry PKI
	**Provider Practitioner** Eg Doctors, consultants, nurse practitioners, nurses. These would be healthcare providers holding registrations with professional bodies. Datasets accessed normally include health information for many people.	Encryption only TLS	Encryption Authentication Captcha	Encryption Multi Factor Authentication Audit	Encryption Multi Factor Authentication Audit Access expiry PKI
	**Provider Care Worker** Unregistered care providers. These would be healthcare providers who do not hold registrations with professional bodies. Datasets accessed would still normally include health information for many people.	Encryption only TLS	Encryption Authentication	Encryption Authentication Captcha Audit	Encryption Multi Factor Authentication Audit Access expiry PKI
	**Machine to Machine** Computers and applications exchanging information. Examples are GP practice management systems accessing the national enrollment service (NES) or a laboratory result providers exporting results into a hospital information system.	Encryption only Unauthenticated APIs TLS	Encryption Authentication within API	Encryption Pre-shared key exchange Firewall IP filtering Audit	Encryption Pre-shared key exchange Firewall IP filtering Audit Access expiry PKI
	**Researcher / Quality Improvement** Healthcare improvement research. Typically would be the Ministry of Health, a District Health Board or a Primary Health Organization but could also include Medical Schools or other health sector researchers.	Encryption only TLS	Encryption Authentication Captcha	Encryption Multi Factor Authentication Audit	Encryption Multi Factor Authentication Audit Access expiry PKI
	**Funding Provider** Typically would be the Ministry of Health, a District Health Board or a Primary Health Organization but could also include health funding providers.	Encryption only TLS	Encryption Authentication Captcha	Encryption Multi Factor Authentication Audit	Encryption Multi Factor Authentication Audit Access expiry PKI

Roadmap for moving from Connected Health the *product* towards Connecting Health the *ecosystem*

- Services currently requiring a legacy Connected Health connection will be identified and classified according to the guide above and then dual-published onto the internet using the appropriate security controls
- New client requests for legacy Connected Health connections will be approved by exception only or for necessity rather than simply by having an HPI number
- Existing clients on the legacy Connected Health network will be required to provide a list of which applications are in use on the network and for what reason.
- New services from health sector service providers will be provided via the internet using appropriate controls as listed above unless adequate justification can made for delivery on a private network.

*** All access and use of health information must comply with the Health Information Privacy Code Rules. Use of data should be guided by the HISO Health Information Governance Guidelines and health sector technology infrastructure should be managed in compliance with the HISO Health Information Security Framework ***

CONNECTED HEALTH → CONNECTING HEALTH: migrating from a private network to a public ecosystem… …and moving from good to great!

An immediate priority for the future of the Connected Health capability is to lift the security maturity of its user community thereby ensuring data, applications and services are accessible by consumers without the need for a special network.
Popular wisdom among the sector suggests Connected Health is both a secure and assured network. In reality, it really is a 'trusted community' on an isolated network.

Therefore, in order to drive improvement in the security of users, data applications it will be necessary to be more prescriptive regarding:

- the minimum mandatory technical security standards and maintenance practices required of *current* Connected Health users [and their connection providers] and
- the minimum mandatory technical security standards and maintenance practices required of *new/onboarding* Connected Health users [and their connection providers] in accordance with a much greater choice of technology solutions that can be leveraged to begin Connecting Health [as per the Connect Health matrix].

Alongside with defining these new standards, added emphasis should also be given to requiring transparent evidence of compliance with these security standards, and the provision of a clearly defined migration timeline towards the achievement of these measures.

This action will create two defined outcomes:

- the existing Connect Health network will begin organically transitioning towards a more secure and assured network and
- those whom cannot/don't want to meet these next Connected Health standards will transition away from the status quo towards the more open solution/standards-defined ecosystem approach envisaged within the Connecting Health matrix.

We are moving to an internet first connection model whilst mandating that appropriate security is in place to properly protect users, data and applications used in the digital delivery of healthcare services.