Introduction

A medical consultation often results in the production of numerous pieces of paperwork, that are handed to the patient and/or posted or faxed to another healthcare provider. In an era where documents can now be created in a digitally format and transmitted electronically the dependence on paper and fax is increasingly anachronistic.

However it is not yet practical to replace paper with a digital exchange. Medical Practitioners are increasingly frustrated with this daily tangible reminder of the lack of progress towards a seamless digital framework. The sudden shift to virtual consultations associated with Covid-19 has exacerbated this frustration, though the move to electronic prescriptions has eased the concern for the most important documents.

Healthcare has not adopted email, which is used in other industries, because of security / privacy concerns (which have regulatory and legal bases), and through the word, healthcare remains the main customer for faxing and other paper based record solutions, even though such paper based exchanges have their own well known security issues.

Australia has spent almost two decades trying to construct a workable digital document exchange system. Technical interoperability has been largely achieved in theory however practical interoperability has not, in that a medical practitioner cannot simply send a document to any practitioner without having to think about it. Instead, they must deal with a myriad of electronic communication channels, using different channels for different providers. This is believed (documented?), to create safety risks which can result in adverse events and death.

Secure messaging should be as easy to use as ordinary email, and as ubiquitous.

There appears to be a collective lack of national desire to resolve these issues, and this is a source of considerable frustration for the healthcare provider community. We are now at a crossroads and need to determine a pathway forwards. The Secure Messaging Process that the Australian Digital Health Agency has been administering appears to have run out of steam without delivering on its original intent.

This document outlines an approach that can solve this problem at scale, while creating an infrastructure that can be leveraged in multiple other directions, and that offers the potential to transform the healthcare process.

Overview

We propose that Australia rapidly migrate to a new architecture, based around current web standards, and built on NASH certificates.

An overview of the system that we propose:

- Each provider puts up a web service on the internet
- Any communications with the web service are secured by a key exchange based on NASH certificates, so that the identity of both client and server in the exchange are proven
- A registry of Australian healthcare service providers is set up. Anyone with a current NASH certificate can query it to find providers
- Anyone can register providers with the registry. When registering the providers, a token must be provided, and this token is used to confirm the registration with the nominated end-point

- Any NASH certificate holder can send a message through the service to any provider registered on the end-point using a push end-point as described below
- In addition to receiving push messages, the end-point can also be a FHIR server and/or provide other services as well (e.g. dicom-web, CDA/XDR, CDS Hooks)
- As part of the payment process, Medicare and potentially other payers check that providers have a current registered end-point that works before paying the provider (after a grace period to get it set up)
- There's a revocation list of NASH certs, and the end-points are periodically checked that they are following the revocation list (else Medicare won't pay)

The key features of this system:

- There is no need for any messaging intermediaries (though commercial service providers still play an important role)
- There is enforcement that everyone is in the system in order to get paid
- The system can be leveraged for future use (including patient messaging and other functionality described in the national digital health strategy)
- There's no need to invest in an administered directory of providers and end-points (this has proved to be an ongoing challenge)

Architecture

The main functions for the end-point:

- The end-point is hosted on a web server and must use a standard SSL certificate using standard web best practices
- The web server hosting the end-point can provide services other than the ones described in this document (e.g. clinical web site, appointment portals etc)
- The end-point uses the SMART backend services profile (https://hl7.org/fhir/uv/bulkdata/authorization/index.html) for certificate exchange. Note the following points:
    - Both client and server must use NASH certificates that identify their HPI-O
    - We will define a specific scope for message delivery
    - See below for application registration process
- All exchanges with the end-point for services described below require the Authorization to happen first. Note that the same end-point could also be a FHIR server providing Patient based OAuth access to other FHIR services (e.g. Australian Argonaut) and these services might not require Nash based certificate agreement, but the services below always require NASH based Authorization unless otherwise stated.
- Services:
    - Provider affirmation – confirm that the end-point is able to receive messages for the specified provider
    - Token Affirmation – given a token and purpose, affirm that the token is valid for the purpose it is being used for (this simple protocol supports other protocols below)
    - Message delivery – send a message, with parameters, and get a result (described below)
    - Also, return a FHIR Capability Statement – return a FHIR capability statement confirming that this is an Australian Health care messaging end-point (and possibly other things). Note: This service (return a capability statement) may be returned using other authentication methods too (e.g. without NASH certificate exchange)

Note: there can be many end-points for a single HPI-O, and even for a single HPI-O certificate, though this latter would be at least discouraged as a matter of security design.

The main functions for the registry

- The registry is an implementation of the existing FHIR based Australian Provider registry specification
- Any access requires authorization using back-end services (as above), using a NASH certificate
- It allows search of providers to all authorised users, as specified in the provider directory specification
- It also allows registration of a provider, with a nominated end-point. The registration must be accompanied by a token which will be confirmed with the nominated end-point when the registration is performed (this process also assures that the end-point is provided by the HPI-O in the certificate). Note: Enforcing proper use of the certificate is the role of the certificate owner

The registry has it's own NASH certificate identifying it.

The standards

- Back end Services: http://hl7.org/fhir/uv/bulkdata/authorization/index.html
- Australian Provider Directory: http://hl7.org.au/fhir/pd/2017Dec/
- Additional lightweight standards are required for:
    - The token exchange protocol,
    - The message delivery / response protocol

The FHIR standard has some candidates for these, but there may be other more directly suitable approaches or standards to use.

Risk Assessment

This system rests heavily on NASH certificates, and on their proper management and security. The main risk is for an attacker to get hold of a NASH certificate and use that to impersonate a provider working for that HPI-O.

Mitigations:

- Enforce that all participants are actively using the NASH certificate revocation list (with an automated police bot – see below)
- if a provider already is registered, then notify a security watchdog and the registered providers for the end point that their registration is changing

A secondary risk is that general problems around NASH certificate registration will erode the functionality and efficacy of the system.

Mitigation:

- This eco-system makes it important to invest in the NASH administrative process

Police bot

The police bot watches all participants in the system, checking that security is maintained and that certificate revocation is being observed. In addition, the police bot maintains a list of providers

whose service is up to date and passing all tests. Medicare checks this maintained list periodically when processing payments. The bot notifies any provider whose end-point has a problem.

Implementation Path

In order to boot strap implementations, we need an open source end-point that anyone can use (can be written), and an open source implementation of the registry. These can serve both as reference implementations for all the other vendors, and also can ensure that all participants are able to minimally participate with the use of an open source end-point provider if necessary.

Obviously the goal is for all the system vendors to write their own integrations into their own software, but delivering open source exemplars will prime the pump for this. Typically, such open source projects also grow into key validation tools that are necessary for a process like this to achieve full maturity.

A project like this could be run as a joint project between HL7 Australia, and the MSIA (Medical Software Industry Association), and moved along with through industry meetings and connectathons. Obviously participation from the state and federal authorities would be a key success criteria, but it is not obvious right now whether there is a path to this.