

Draft HealthConnect Business Architecture consultation June 2002
Submission #11 – National Office for the Information Economy



NOIE

The National Office for the
INFORMATION ECONOMY

*A proposal by the National Office for the Information Economy, in
response to the draft HealthConnect Business Architecture,
published by the HealthConnect Board in March 2002*

This paper has been produced for consideration by the Board of HealthConnect and for use by the Board in pursuing the objectives of HealthConnect, Canberra, June 2002

Managing health data - a proposal

Purpose of the paper

The National Office for the Information Economy (“NOIE”) has prepared this paper to provide a conceptual view of a national framework that would meet the objectives of the HealthConnect project and other significant policy objectives.

The paper proposes a high level model within which HealthConnect can devise and implement an effective and efficient national health information network. It is not the intent of this paper to prescribe technical or other solutions.

The proposed model is scalable both in *depth* – the quantum and level of data managed – and in *breadth* – the scope of data managed. The model could be extended to encompass all government data, as shown in Figure 2.

The model accommodates the fundamental components of HealthConnect, as described in the Overview of the Draft HealthConnect Business Architecture¹.

Context

NOIE is the Federal Government’s lead agency for information economy issues. NOIE provides strategic advice to Government on the key factors driving the information economy and, in this context, coordinates the Government’s *Strategic Framework for the Information Economy*².

The Office promotes the benefits of the information economy, acting as a catalyst for change in the wider community and focusing debate on the use of new information tools in the Australian economy. NOIE also coordinates the application of new technologies to government administration, information management and service provision.

The Office is helping Australians create a world class online economy and society through its work coordinating Commonwealth Government responses to the information revolution.

The health industry is significant in terms of its size and its capacity to improve the lives of all Australians. It is also a major user of new information and communication technologies and a driver of change in the innovative application of these technologies to business and therapeutic objectives.

For these reasons, NOIE believes that the HealthConnect project is very important and merits NOIE’s full support and collaboration.

The authority for the HealthConnect project is derived from the National Health Information Management Advisory Council (NHIMAC). Australian Health

¹ Pp. 8-9, Version 0.7, Canberra, March 2002.

² See <http://www.noie.gov.au/projects/information%5Feconomy/strategic%5Fframework/index.htm>

Ministers established NHIMAC in April 1999 as the peak body for progressing significant issues regarding the use of information in the health sector.

NHIMAC's main role is to advise Australian Health Ministers on information policy and use of new information technologies in the health sector³. This includes:

- providing Health Ministers with options for promoting a nationally uniform approach to achieving more effective information management within the health sector;
- promoting the efficient and effective use of information technology in health;
- developing a partnership with the private health and information technology sectors;
- encouraging the development of a market for Australian health information technology and services; and
- protecting the public interest, particularly in relation to privacy.

Members of NHIMAC represent Commonwealth and State and Territory Governments, clinical practice, the information technology industry, the private health sector and consumer interests. The Federal Privacy Commissioner is a member, as is the Chief Executive Officer of NOIE.

NHIMAC has produced *Health Online: A Health Information Action Plan for Australia*. This is a national strategy for information management and the use of online technologies within the health sector and a set of action plans for nationally significant and State and Territory projects. The plan promotes new ways of delivering health services that benefit consumers, by harnessing the potential of new technologies.

The innovative ways to manage information proposed in *Health Online* are aimed at building a better health system that will benefit those who use it - health consumers - and those who work in it - health care providers, policy makers and managers. It will also benefit businesses that support the clinical and service delivery process, such as health insurance funds.

Health Online is about empowering consumers by providing them with greater access to information about their health as well as about treatments or interventions and any side effects. It will help them to make considered choices within the health system and provide the opportunity to exercise more control over their own health and wellbeing.

Health Online includes projects that promote the availability of online health services. These projects provide exciting opportunities to increase consumer access to a range of health services. One of these projects is HealthConnect.

³ See <http://www.health.gov.au/healthonline/welcome.htm>

Linking with HealthConnect

The HealthConnect model (see below) is intended to test ways and means to provide Australia with better management of health data and records. HealthConnect has published a draft view of what a voluntary national health information network might look like – a “business architecture”- and has asked for comment on the draft.

The HealthConnect Business Architecture is an essential component of the HealthConnect research and development (R&D) project. The Business Architecture describes how HealthConnect will deliver on its objectives and it will underpin any testing of the concept on the ground.

The intent is that health-related information about a person would be compiled in a standard electronic format at the point of care, such as a hospital or a general practitioner's surgery. It would then be stored as part of a secure electronic network, with the permission of the person receiving the care.

This information could be retrieved online, via the network, whenever it is needed and it could be exchanged between authorised health care providers - again, only with the consent of the consumer.

Policy objectives: HealthConnect and beyond

The policy objectives of the HealthConnect project are to improve the efficiency and effectiveness of information flows in the health system and to protect the integrity of personal information stored within the health system.

The Commonwealth Government has other, related policy objectives that depend on access to clean, reliable, complete data sets. These are:

- To improve the efficiency and effectiveness of government business processes.
- To prevent and detect identity fraud and related criminal activities.
- To lift the level of community confidence in e-business and in e-commerce.

Background

Managing health data in Australia, as in other developed economies, is a complex problem or, rather, a set of interrelated, complex problems.

HealthConnect was established to address this set of problems, within a broader plan - *Health Online: A Health Information Action Plan for Australia* (<http://www.health.gov.au/healthonline/welcome.htm>).

The purpose of HealthConnect is described thus⁴:

⁴ From http://www.health.gov.au/healthonline/hc_1.htm, accessed on 3 June 2002.
National Office for the Information Economy 13/11/02

“To achieve such benefits, the National Electronic Health Records Taskforce has proposed the concept of a voluntary national health information network (HealthConnect) that would allow information held in electronic records to be collected, safely stored and exchanged within strict privacy safeguards. This process could only happen with the individual consumer's permission.

Under HealthConnect, a person's health-related information would be collected in a standard, electronic format at the point of care (such as at a hospital or a GP's clinic). This information would take the form of health summaries, rather than all the notes that a health care provider may choose to keep about a consultation.

With the consumer's consent, these summaries would then be able to be retrieved at any time they were needed and exchanged via a secure network between those particular health care providers authorised by the consumer to access this information.”

The development of this paper has been shaped by many sources, including a program run by the Irish Government, called *Reach* (<http://www.reach.ie/index.htm>).

At the heart of *Reach* is the role of Public Services Broker. This electronic broker acts as a helper or assistant between clients/customers and Public Service agencies. The role is being developed by *Reach* and will then subsequently be operated by a separate agency.

The Public Services Broker will provide a single mechanism for access to public services to improve service delivery through traditional means (in person and on the phone) and new self-service electronic channels⁵.

Guiding principles

The principles guiding the development of the model discussed below are:

1. The fundamental elements of HealthConnect should be accommodated.
2. The management of personal (health) data should not be a service provided exclusively by government.
3. The Commonwealth Government should be responsible for the provision of a national framework of trust, covering privacy, security and authentication.
4. The Commonwealth Government should have the responsibility to regulate the collection, management and access to personal data.
5. The individual should control his/her data, by setting parameters for access.
6. National data standards should apply (covering both technical and management requirements)⁶.

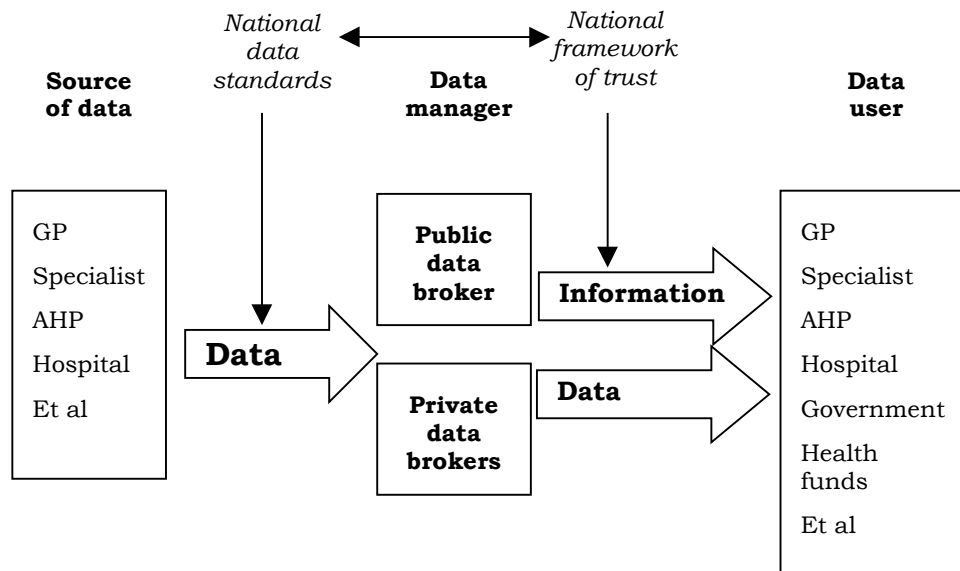
⁵ From <http://www.reach.ie/about/psb.htm>, accessed on 3 June 2002.

7. National privacy standards should apply.
8. Protection of individual rights established by these principles should be universal.
9. Access to data by service providers should be universal and ubiquitous (subject to 2).
10. Risk and risk management should be scalable.

The model

The proposed model is shown below (Figure 1)⁷.

Figure 1: A model to manage health data



A national regulator would oversee the system, giving effect to the principles underpinning a *National framework of trust*: protecting privacy, ensuring security, and enabling authentication. The regulator would oversee the operations of the data brokers, issue licences, conduct audits, impose sanctions and so on⁸.

The regulator could be an industry specific regulator or an existing regulator whose mandate could be adapted to this purpose.

The individual (citizen/client/customer) would choose the data manager and, within the national standards, would prescribe the depth and breadth of access

⁶ The groundwork has been done, see <http://www.health.gov.au/healthonline/sp/standards.pdf>

⁷ Information is data + meaning, see MH Boisot *Knowledge Assets: Securing Competitive Advantage in the Information Economy*, Oxford University Press 1998.

⁸ This would assist in the prevention and management of identity fraud, which is a significant problem, see *Scoping Identity Fraud*, by Geoff Main PSM and Brett Robson, Attorney-General's Department, Canberra, September 2001.

to personal data. The individual would be able to choose the public data broker or a private broker to hold and manage his/her personal data.

The public broker would provide a universal service. That service would be free to the user or impose a minimal cost on the user. The public broker would ensure that everyone in Australia has the level of privacy protection mandated by Parliament and would facilitate fair and equitable access to government services through the management of personal data.

The private broker(s) would provide a user pays service, adding value to the fundamental services provided by the public broker. For example, a private broker may provide customers with a smart card that tracks data of particular interest to the customer and that could be used to manage expenses or a health care plan (or anything the customer wishes). A private broker could also operate a linked health fund or insurance service.

With any broker, the individual customer would decide what data goes to whom and for what purpose.

Within this model personal data could be stored in a distributed or centralised mode or through a mix of these modes. These are decisions to be made later, once a national framework has been agreed.

Ownership, control and beneficial use

To understand this model, it is important to distinguish three types of relationship one may have with personal data. This is best done by using an example.

A general practitioner (“GP”) is likely to have *records* that include personal *data* (and information) related to many individuals. The GP *owns* those *records* and is responsible for them. That would not change under this model. However, each individual would have the right to determine what the GP may or may not do with the data and information pertaining to him or her, giving the individual *control* over personal *data* owned by the GP. The only exceptions to this would be a medical or other emergency or judicial intervention.

If the GP is of the view that a treating specialist needs to know certain elements of personal data, it is the GP’s role to explain to the patient why this is so and to obtain appropriate consent. Blanket or generalised consent could cover most circumstances, but may not cover all circumstances. If the GP and the individual disagree on what should be accessible to whom and cannot or will not reconcile their views, each has the right to end the relationship at any time.

This way the GP remains in control of his or her professional practice and can exercise due diligence, while the individual (the patient) retains control over information that belongs to him or her. The integrity of the doctor/patient relationship is preserved.

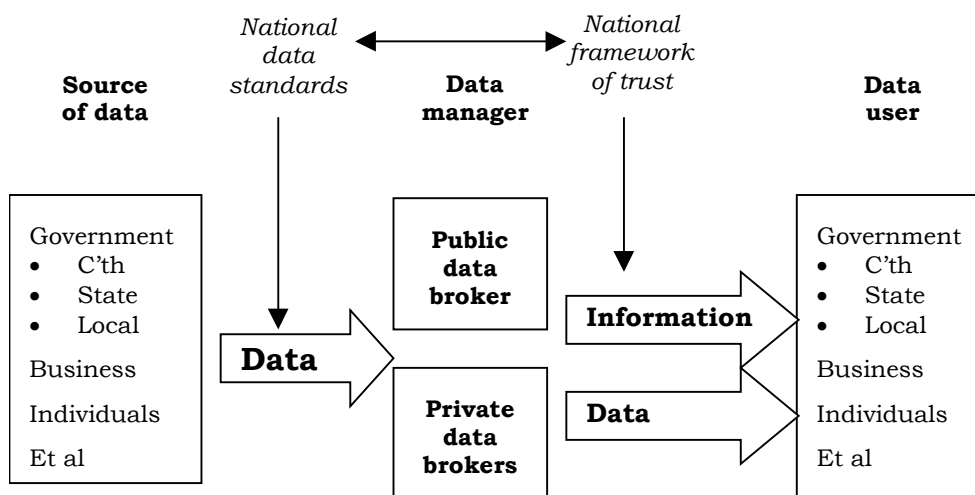
While the GP may own the data in question and the individual may have control over the data relating to him or to her, many parties may have *beneficial use* of the data.

These may include others who are involved in caring for the individual's health, health insurers, government agencies such as the Health Insurance Commission and so on. Also, aggregated data may be used by government, universities and others for research, planning and management purposes.

Possible extension of the model

As alluded to earlier, the model shown at Figure 1 could be expanded to encompass a greater range of data held by government and, potentially, all data held by government, at all levels. This expanded model is shown at Figure 2⁹.

Figure 2: A model to manage government data



Standards for data protection

Within the proposed model (Figure 1) there are two types of transaction envisaged:

1. Between the individual and the data broker.
2. Between the data broker and the provider or recipient of data.

The individual's transaction with the broker is akin to the relationship s/he may have with a provider of financial services and an appropriate level of security should apply. This could be done by means of a personal identification number ("PIN"), a password or a combination of such tools. This would provide adequate protection and trust at a relatively low cost.

⁹ See note 7.

For the second type of transaction, a higher level of security is required, akin to bank to bank transactions. Here it would be appropriate to mandate a basic level consistent with public key infrastructure (“PKI”), although alternatives such as SPKI/SDSI or Brandsian Private Credentials may be preferable¹⁰.

Summary

The concept proposed here:

- is a simple, flexible framework that would accommodate existing and new technical solutions;
- places control of personal data in the hands of the citizen/client/customer, while allowing others to have beneficial use of the data;
- allows government access to clean, reliable, structured sources of data;
- allows health providers to manage data efficiently, while protecting the integrity of the clinician/patient relationship;
- provides a national regime of privacy protection that is available to all, at no direct cost;
- lessens the risk of identity theft or fraud;
- creates a new market, with new business opportunities;
- and also creates a risk management gradient – adequate protection for all, user pays for those who want more; simple security tool for the individual, higher level of protection for data at industry level.

¹⁰ See “Why Do We Need PKI? Authentication Re-visited”, by Roger Clarke (2002), at <http://www.anu.edu.au/people/Roger.Clarke/EC/PKIRW02.html>, accessed on 12 June 2002.
National Office for the Information Economy 13/11/02 8