

# Sharing Health Data: Privacy & Trust

---

Peter R Croll and David P Hansen

## 1. Introduction

Patient information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule but it applies in most circumstances. In general, patients entrust their Health Service provider to allow them to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust.

This data however could be used for a second purpose; it could be combined with data from other patients to allow researchers to perform population based studies. This secondary use of data is explicitly permitted in some circumstances but is often viewed as a legal and ethical minefield. However, for medical researchers and health service providers it could provide valuable information on things such as cause of the disease and best treatments or the patient journey and disease clusters.

For such secondary usage to be accepted to data custodians and the community in general, they must understand the risks that data sharing exposes. To date, most data has been collected and stored as manual records but the increase use of electronic records introduces new risks, particularly from the remoteness and speed of access that is now achievable. Appropriate use of technology can reduce the risks of incidences associated with common security weakness. Whatever methods are used the software products must operate in a particular environment with particular external impacts resulting in a unique set of interconnected hazards and problems. Consequently, the associated risks are highly application dependent and the risk management must be highly customised to suit. Health data spans across numerous databases and jurisdictional boundaries. Hence, there is a need for joint agreement on the business process utilised such that any technical solution adopted will need to be driven by these processes and yet flexible enough to suit the differences at organizational, state and federal levels.

## 2. Privacy and Trust: Australian Context

The Australian National Privacy Principles in the Privacy Amendment (Private Sector) Act 2000 [1] define 10 principles which cover a range of issues associated with data collection, data quality and security, the movement and access of data and personal identification from sensitive information. From 21 December 2001 health service providers covered by the federal Privacy Act have needed to comply with these ten privacy principles that allow for individuals to exercise new rights and choices about how their personal and health information is handled in the private health sector.

Within Australia various states have enacted their own specific legislation relating to health and privacy. For example, in Victoria the Health Records Act 2001 regulates the handling of health information by any organization in the public and private sector, and in the ACT the Health Records (Privacy and Access) Act 1997 applies to all records of kept by public and private sector health services. Other states, notably NSW, are also looking at developing specific legislation in this area.

In order that research can continue to inform and improve Australians' health while complying with the Privacy Act, the National Health and Medical Research Council has issued guidelines [2] approved by the Privacy Commissioner. These guidelines balance the protection of an individual's health information with the need for ethically approved research using individuals' health data without consent.

### Static v Dynamic Risks

Regardless of the guidelines there are some real risks to collecting and using sensitive health data. These include the risks faced by data custodians in not following the privacy principles and their local policies, in particular, the disclosure of individuals and the incorrect use of data. Other risks include the

loss of trust that the providers of data, i.e. the patients, have in the IT systems we use. That is, the ability to use patients' data for research without their consent is irrelevant if their trust is eroded and hence they don't participate in providing the necessary data. For any given system these are often static risks that can be estimated and minimized.

With the increase push toward national health data integration such as Health Connect [3] and the problems of differing state and organizational policies, these risks are far from static. The National e-Health Transition Authority state that privacy protection in Australia is a complex patchwork: "NEHTA's position has been to chart health privacy requirements within the privacy environment that we have now. It is considered possible to navigate the existing privacy environment although this is not without some risk and may require future changes" [4]. Hence, any policies that data custodians follow need to be flexible and updated on a regular basis to allow for these changes.

### 3. Building trust for HDI™

Health Data Integration (HDI™) is a powerful software tool [5] that underpins the linkage of critical information across disparate database sources, for example, CSIRO's Preventative Health (p-Health) Flagship. The primary goal of p-Health is to save significant direct costs in health care with chronic diseases being the main target. HDI™ has the capacity to provide unique insight into possible causes and effective prevention methods through extensive population studies of collected health data. This data is dispersed across several data bases with many custodians responsible for its integrity and privacy. The architecture of HDI™ is being developed to provide state-of-the-art in robust security technology and flexible access control mechanisms. This has to be coupled with the privacy requirements to limit the movement and access of identifiable data yet at the same time permit matching of records to facilitate research. In the handling of sensitive information, trust is a critical factor that can take years to build and a moment to break. The successful outcome of HDI™ and the p-Health program relies on building and maintaining such trust against a backdrop of shifting policies on data protection.

### 4. The way forward

Our aim is to understand the business processes in order to support the sharing of health data. We will take a novel approach to investigate if the risks to both data privacy and security have been minimized to acceptable levels. If programs like p-Health are to meet their primary goal, this is crucial; it will help ensure that the essential trust of the data custodians and providers cannot be readily or unintentionally eradicated. The protection and integrity of health data is an active area of research with many differing approaches taken to deal with complex issues involving government privacy policies, patient consent, unique identification, secure messaging, data matching, depersonalization, etc. Ongoing work on standards continue with the ambitious aim of establishing unifying approaches, e.g. the National e-Health Transition Authority. Numerous divergent approaches continue to be researched aiming to provide practical, secure and compliant solutions to health data privacy. Convergence towards a viable universal solution is not imminent therefore trust in e-Health is decidedly more fragile as compared with many other industry sectors.

### References

1. Privacy Amendment (Private Sector) Act 2000, <http://www.privacy.gov.au/publications/> Sept 2005.
2. NHMRC (2000) Guidelines (s.95 and s.95A), Under Section 95 of the Privacy Act 1988, published by National Health and Medical research Council, Reference No: E26, 2000
3. Health Connect (2004) Fact Sheet – HealthConnect, [www.healthconnect.gov.au/about/Fact.htm](http://www.healthconnect.gov.au/about/Fact.htm) Sept05.
4. NEHTA (2005) The National E-Health Transition Authority, [www.nehta.gov.au](http://www.nehta.gov.au) accessed Sept 2005.
5. DP Hansen, C Daly, K Harrap, J Jacquet, MA O'Dwyer, C Pang, J Ryan-Brown (2005) Health Data Integration : Research Software to Commercial Product, Australian S/W Eng. Conference, ASWEC 05.



ICITCC 05 Abstract Submission  
Prof Peter Croll



Dr David Hansen