The privacy imperative for a successful HealthConnect

Malcolm Crompton

As part of the Australian Government’s MedicarePlus initiative, a roll-out of the national electronic health records (EHR) system, HealthConnect, is to begin in Tasmania and South Australia from July 2004.

Reflecting the importance placed by the community on the privacy of health information, the Office of the Federal Privacy Commissioner (OFPC) has maintained a strong interest in the development of HealthConnect (see, for example, OFPC 2002). Most recently, in February 2004, the OFPC made a submission to the HealthConnect Project Office on its Interim Research Report and Draft Systems Architecture for HealthConnect (OFPC 2004a). This submission, available from the OFPC’s website at <www.privacy.gov.au>, argues that work remains to be done to ensure adequate privacy protections are in place for HealthConnect.

The potential benefits of well designed, implemented and managed electronic health records systems are difficult to dispute. HealthConnect is conservatively expected to deliver financial savings to the health sector of at least $300 million per year (HealthConnect 2003a), as well as facilitate improved electronic linking of health information for clinical and health research purposes (see, for example, Stanley 2003). Most importantly, it may improve clinical treatment by enhancing information flows between health service providers.

In recognising these potential benefits however, it is essential to pay equal attention to the risks of such a system, including those which might undermine its very success. HealthConnect would vastly increase the capacity to collect, store, copy, transmit, share and manipulate health information, and perhaps in ways not expected by individuals. There is increased potential for health information collected for one purpose to be taken out of context and disclosed for other purposes incrementally less related to the reason for which it was initially collected (the function creep phenomenon, discussed recently in the context of identity management [OFPC 2004b]). This potential is enhanced by the IT-enabled ability to link data from currently disparate sources, possibly including those from beyond the health sector.

If HealthConnect is to meet its objectives, which are partly reliant on achieving a significant critical mass of participants, then it must inspire the trust of the Australian community that personal health information will be kept private. It is axiomatic that individuals’ willingness to engage in the health sector may be affected by their perception of how their personal health information will be used and how much control they have over it. A HealthConnect system that does not engender trust may result in individuals withholding important health information from providers or, in some cases, avoiding medical treatment altogether (Cavoukian 1999; Goldman & Hudson 2000). Accordingly, rather than an obstacle to be mitigated, privacy is a fundamental necessity for an effective EHR system.

Individual control: informed, voluntary choices

Essential to the achievement of trust in individuals is their control over their own information, and this includes choice as to whether they participate in the system at all, and, if they chose to do so, the extent of their participation. The OFPC welcomes the ongoing commitment to informed and voluntary participation in HealthConnect, whereby an individual makes an active decision to opt-in to the system.

However, choice also entails offering options, so that an individual can determine the extent of participation for a given health-service event. In this regard, the Tasmanian fast-track trial does not go quite far enough. In particular, the early evaluation finding that “Consumers are not yet empowered to control the extent to which their information is being shared between participating providers” is of concern (HealthConnect 2003b, p.3).

A more responsive form of consent framework, described as layered-consent, has been proposed by the OFPC. Readers of this journal may recognise this proposal as similar to the model proposed in the UK and known as the sealed envelope. This offers to individuals the choice for particularly sensitive information to be accessible only to nominated providers, who can see the sealed envelope, thus affording a greater degree of control over their information. This would seem to achieve a pragmatic approach to consumer consent without sacrificing adequate choice and control for individuals. An opt-out arrangement is simply not good enough, having the potential to disempower consumers and provide insufficient range of choice.

Accountability and oversight

Also essential in gaining community trust is an accountability and oversight framework, whereby:

- The Australian community is told clearly what the system is intended to do
- The system, once implemented, does what is intended and nothing more or less
- The system operates in an open and accountable way, by way of audit and mandatory reporting, to demonstrate that it is continuing to meet its commitments.

To achieve this, it is necessary that powers regarding the functioning of the system (that is, the management of the system) should be separate from powers of oversight (independent accountability). The oversight body setting the rules for matters such as access and consent arrangements should be separate from a necessary, independent complaints handling body.

System implementation

Two implementation elements that must be addressed prior to HealthConnect roll-out are, first, that a full evaluation must be performed on appropriate, scale-
able trials; and second, robust and reliable identification mechanisms must be established. I strongly oppose appropriating the Medicare number as a HealthConnect identifier, a purpose for which it was not designed and is ill equipped. As I argued in a recent speech, it is essential that we get identity management right (OFPC 2004b); the Medicare number does not achieve this.

Technology and law

Finally, the questions of technology and law warrant attention prior to roll-out. While selecting existing technology has obvious immediate appeal, it is arguable that a system as significant and potentially beneficial as HealthConnect justifies the investment required to explore cutting-edge solutions. Privacy enhancing technologies may offer 21st century alternatives with better outcomes (see, for example, Burkett 1998; Cavoukian 1999). Suitable technologies are being developed; arguments that it is not possible are not valid (OFPC 2004b).

The importance of building privacy into technical design is vital. While law is necessary, including, for example, the still emerging AHMAC National Health Privacy Code, it is largely limited to addressing what should happen, rather than ensuring what can happen. Technology and law are essential co-requisites to a HealthConnect system that can be trusted by the Australian community.

Given the momentum that this project has acquired, it is timely that the privacy implications of such systems are discussed widely, and I applaud the Health Information Management Journal for contributing to this process.

References


Malcolm Crompton
Federal Privacy Commissioner
Office of the Federal Privacy Commissioner
GPO Box 5218
Sydney, NSW 2001
Tel: +61 2 9284 9671
Fax: +61 2 9284 9666

Malcolm Crompton’s term as the Federal Privacy Commissioner expired on 19 April 2004.