

Thank you for the invitation to comment on the ‘Draft HealthConnect Business Architecture’, dated March 2002 (‘the Draft BA’). I welcome the opportunity to make a submission on a major component of the design and implementation work stream of the HealthConnect Project.

The Draft BA document indicates it will be the first of several drafts of the HealthConnect Business Architecture during the two-year HealthConnect research and development project. The Draft BA has been developed prior to, and independently of, a number of other significant HealthConnect project components and systems, including the key privacy policies around consent and access control.

In this context, the comments I provide are necessarily provisional given that so many other aspects of HealthConnect are yet to be carefully considered. I envisage an opportunity to provide further comments on the privacy aspects of the Business Architecture and HealthConnect, particularly once the HealthConnect systems can be seen as a whole. Only at that time, will I be in a position to provide comment on whether or not HealthConnect can offer a framework and arrangements that enhance the privacy of individuals, while at the same time delivering an on-line health system.

A cohesive HealthConnect system and privacy ‘building blocks’

The Draft BA has been designed to ‘house’ the functions of the various internal systems and provide the necessary functional framework for HealthConnect as a whole. Privacy is identified as one significant ‘building block’ and it is keenly recognised in the HealthConnect and HealthConnect Project’s guiding documents, such that ensuring the protection of an individual’s health information will be important in attracting viable numbers of participants. Once trust in a cohesive system has been established, this will ultimately attract participants. Therefore, it is vital that the final Business Architecture is one which describes and creates an environment where privacy is fundamental to the fabric of the system.

The success of HealthConnect will depend upon the coming together of an identified series of interrelated activities and systems. In our view, given that some of the systems of HealthConnect are being created disparately and independently, there are significant issues with overall cohesion. We know that many elements of the system, such as the models around consent and access control, individual patient identifiers and software programs, which are pivotal to protecting and enhancing individuals’ privacy, are still in design. The Draft BA refers to these elements, but given their disparate development, it is yet not meaningful to offer comment about the system as a whole.

This includes, for example, the considerations proposed for consumer registration (p: 76) and consumer identification (p: 77), upon which we cannot provide overall comment.

I draw your attention to a specific concern about the impending ‘fast track’ trial sites. The Overview document (p: 24) discusses the HealthConnect trial sites and says that privacy protocols will be in place before going ‘live’ at these designated sites. The Draft (p: 16) outlines how the trials are to provide feedback about various systems in order to be evaluated for efficacy. Two trials, however, are being ‘fast-tracked’ and are due to go live in September 2002.

At this stage, the privacy protocols for these trials are still in development. Also, proposed consent models that emerged from a national workshop on consent appear not to be intended for use as part of the trials. This Office provided similar comments to the Department directly in relation to the Trial Site for Tasmania. This seeming lack of integration illustrates our concern about the Draft

BA and its relationship to the project overall. It is my strong view that HealthConnect must eventually work to combine and effectively integrate (and clearly communicate the integration of) all instrumental elements before securing its final approval as a national electronic health system.

Consent

Since December 2001, the *Privacy Act 1988* (the Privacy Act) has protected the health information of individuals held by private health service providers nationally. The December enactment recognised the special status of health information and provides greater control for individuals over the handling of their information. The intent of the legislation is encapsulated by the phrase “My Privacy. My Choice.”

Fundamental to the notions of choice and control is the concept of consent. Where individuals are provided with a framework and arrangements empowering them to make fully informed choices about the handling of their health information, they will have greater confidence in the protection of their information, and are more likely to participate in the HealthConnect system.

The importance of getting the consent arrangements right cannot be overstated. In this context, we mention the following points:

- consent has been acknowledged, through the Draft BA, as being important. There are many occasions, however, where issues of cost are highlighted when discussing consent models and computer applications. The Draft BA, for example (p: 142), raises concerns about the viability of ‘consent’ and that, depending on the model constructed, this may increase the cost exponentially. Privacy has been identified as a guiding principle and a fundamental ‘building block’ to the HealthConnect project, so cost-effectiveness must be seen as only one of a number of considerations - indeed given its pivotal role in HealthConnect, it may not be the critical consideration. Given the apparently huge cost savings and other benefits that could be generated by HealthConnect, investment in consent options that genuinely protect and enhance privacy are likely to be highly justified, if not critical, in winning the public support necessary to realise those benefits;
- there is a need to ensure that consent models are not “onerous” for individuals but still give full and meaningful choice and control to the participant (p: 28). A good model will balance the need for flexible arrangements (including options of simple and pre-formulated consent arrangements that can be selected by individuals, as well as options that can be designed by, or tailor-made for, the individual) with the need for acceptability as part of a good business case;
- the emphasis on gaining individual consent needs to be undertaken in ways that are culturally sensitive given the make-up of our contemporary society. This will include ensuring appropriate consent arrangements for indigenous communities, people from a non-English speaking background, people with a disability and the elderly;
- the Draft outlines many occasions where consent may be overridden, and in these circumstances by whom. One such example is in an emergency situation. We suggest that clear advice about who has the potential to override the consent mechanism, and in what circumstances, be made explicit to individuals prior to registration with HealthConnect. More generally, as we do not know the content of the ‘Systems Architecture’, we suggest that whichever consent model is chosen, participants are fully informed of the range of

circumstances in which their consent may be overridden (or not sought) when a data transfer or use is to occur.

Disease Registers and ‘Trigger Rules’

The Draft BA makes a clear assumption that *HealthConnect* will upload to, and download from, a range of disease and other registers (e.g. Diabetes Register, Childhood Immunisation Register etc). The Draft BA discusses the use and development of ‘Trigger Rules’, whereby a programmed ‘alert’ is automatically created after a prescribed disease has been entered into a certain field on the *HealthConnect* screen. These alerts will ‘trigger’ the system’s communication with the relevant database.

Not all disease and other registers are the same in purpose or in their legislative basis, if any. As far as we know, some registers require compulsory notification by or under law, while others are voluntary; some have statutory requirements of consent and provisions setting out privacy protections, while others do not; some are ‘official’ and others seem to be ‘informal projects’; some require identified data, while others use de-identified data. It is, therefore, not possible to describe or create a single set of rules about how these registers will interact with *HealthConnect*. It will be necessary for the system’s software design to be able to recognise and accommodate the various types and operations of registers, so that appropriate triggers are created.

We are concerned about how the development of these ‘Trigger Rules’ will occur and the potential for ‘function creep’ with regard to their operation. Where diseases are notifiable by law, it appears appropriate that statutory provisions be made for corresponding ‘Trigger Rules’. Any subsequent changes to the rules or proposed expansion to the types of diseases and alerts to registers must occur through amendment to legislation. For diseases that are not notifiable, in our view, this kind of ‘alerting’ activity requires consumer consent, either at registration or as a relevant event or change in circumstances arises (p: 25; 95).

The above matters (of consent and systems alerts) may best be considered in the context of the *HealthConnect* Systems Architecture, so that technological design itself enables these privacy protection practices, and prevents attempts to bypass necessary privacy safeguards. It is the combination of regulation (which specifies what should and should not be done) and technology (which controls what can and cannot be done) that will determine whether *HealthConnect* is well designed and enhances privacy. Again, it is not possible to be conclusive about the protection of privacy, in this context, until aspects such as these can be seen as part of the overall system.

The privacy regulatory framework and the governance of *HealthConnect*

In the Draft BA, the authors have anticipated the development of specific legislation for *HealthConnect* – including provisions relating to *HealthConnect* operations, consumer consent, access, provider obligations, and the specific uses of data. The Draft BA sets out the intention to establish two *HealthConnect* Authorities to define policies and protocols, to approve some health information disclosures (to health care providers and researchers) and to monitor information flows. I assume that these Authorities or others, or some other part of the system (this needs to be specified) will be responsible for the effective day-to-day management of the various discrete internal systems and processes, including overall data integrity, overall data security and patients’ requests for access to their data.

It is important to distinguish between the role of everyday management from the separate oversight and accountability functions performed by an independent regulator, such as the Office of Federal Privacy Commissioner with regard to privacy aspects of the system. This distinction between roles and the existence of an independent body is a fundamental accountability measure for a system such as HealthConnect, and is of importance to consumers.

Conclusion

Considerable work has been undertaken so far in the Research and Development phase of HealthConnect. It is our view that there is still considerable work to do. Our strongest suggestion is the need to ensure the effective bringing together of the hitherto separate elements. We suggest that information around the 'building blocks' of privacy, access and consent (and relevant functional details) are included in further drafts of the Business Architecture, along with explanations of the technical and operational requirements and developments that will achieve these functions.

We acknowledge that these elements are more intricate and detailed in essence. It is critical however, that in the development of technical and operational activities, and the core HealthConnect sub-systems overall, the co-ordination and integration of these core elements is closely monitored and tested and their viability (including in relation to privacy) ensured.

Each of the 'building blocks' mentioned are pivotal to the eventual endorsement and acceptance of the next phase of HealthConnect by this Office. As explained earlier, we cannot yet make more fulsome or broader comments on the Draft BA and look forward to providing comment on a more integrated version of the document during the development of HealthConnect.

Yours sincerely

Malcolm Crompton
Federal Privacy Commissioner

22 July 2002

Please note that this submission has had two short & confidential sections removed to allow for publication.