

HealthConnect Business Architecture

Attachment A – HealthConnect Consent Principles and Possible Models

Version 0.7

March 2002

Introduction

This document is an extract from a larger discussion paper on consent being prepared in the HealthConnect Program Office. The purpose of this document is to describe the policy framework for HealthConnect and to describe some of the possible models for consent that will be examined in the trial sites.

Consent and access control – A policy framework for HealthConnect

In this section, a number of possible consent and access control models for HealthConnect are proposed.

Firstly, the underlying principles and features of the consent and access control policy are summarised. These have been identified based on initial consultation undertaken with consumers and providers, and on the recommendations of earlier research in this area.

There are two sides to the consent framework:

1. obtaining consent from consumers; and
2. ensuring access controls for providers reflect the consent given.

These two elements are directly related. That is, what the consumer consents to (in terms of who should have access to what information) must match the level of access a particular provider has to that information.

Both consent and access control elements of the policy framework are discussed below.

8 Consent policy framework

The key principles underpinning the HealthConnect consent policy are that:

- participation in HealthConnect is voluntary and informed; and
- a person will be able to control who has access to what information about them, in accordance with the agreed privacy framework for HealthConnect.

Other minimum requirements include:

Draft - For Comment

- a consumer can choose whether or not a particular event will be recorded on *HealthConnect*. A person may request, for example, that particularly sensitive information, not be recorded on *HealthConnect*;
- consumers will have access to both their own records and to the audit log showing which providers have accessed their information;
- there needs to be a facility to ensure a person can consent on behalf of another person in certain situations;
- the way in which consent is obtained needs to be clear and relatively easy to operate for both consumers and providers; and
- a person can withdraw from *HealthConnect* at any time. For example, a child who was registered on the system by his/her parents, may decide not to continue with *HealthConnect* when he or she is older. While the person's record would not be fully deleted from the system, for future health and/or legal reasons, the record could be set up so that it is no longer accessible to any providers.

The policy will allow a person to consent to:

- any providers involved in his/her treatment and care having access to relevant information, or
- types of providers involved in their treatment and care having access.

Other features of the consent policy could include:

- individuals having the capacity to 'mask' sensitive information, and limiting access to this information to specified providers. This could either be information about a particular health event, or a particular type of information such as sexual or mental health information;
- only specified individual providers having access; and
- relevant information about the individual will be available to providers in an emergency situation, including any 'masked' information.

9 Access control policy framework

The access control policy must achieve two key objectives:

- allow providers to access information about individuals, where the individual has consented to this, in a timely and efficient manner; and

Draft - For Comment

- prevent providers accessing information which they do not have authority or reason to access.

The access control policy will ensure that the authority for a provider to access information is consistent with the consent given by the individual.

Mechanisms needed to control access are likely to include:

- binding rules and legislation outlining what is appropriate collection, use and disclosure of individuals' information. These would be based around existing principles in relevant privacy legislation and the draft AHMAC National Health Privacy Code, which allow for the use and disclosure of health information where necessary to provide a health service to the individual or for other specified purposes. Additional rules will be developed to apply specifically to activities of *HealthConnect*;
- penalties for unauthorised access or misuse of information;
- audit trails and monitoring of access;
- a governance structure that establishes clear lines of accountability and responsibility both for *HealthConnect* oversight bodies and for provider organisations registered with *HealthConnect*;
- limiting access based on the type of 'views' or report format that is relevant to a provider's type of work. This might depend on both the type of provider and where they work. For example, whether the provider is a nurse in emergency care, a GP in private practice, a hospital physiotherapist or radiologist;
- other technical features and mechanisms that control who has access to what information; and
- organisational controls, such as training strategies, staff responsibilities and policies implemented at the organisation level, all of which aim to promote a privacy-aware culture.

The combination of policy, organisational and technical mechanisms needed to control who has access to what information on *HealthConnect* should not be so onerous that they impact on the effectiveness of the system. On the other hand, they need to be sufficiently stringent so that security and privacy of information on the system is assured.

The aim should be to avoid unauthorised access or misuse of individuals' health information, as any breaches of security or privacy may not only result in damage to individuals involved, but to the integrity and reputation of the system as a whole. Where access errors do occur, there needs to be clear lines of accountability and follow up procedures in place.

The types of access control mechanisms listed above include both deterrence measures and technical barriers to access.

Key questions for the HealthConnect access control policy are:

- To what extent can the HealthConnect rely on deterrence measures (such as penalties for misuse and audit trails) to control access to information potentially available on the system?
- To what extent is it necessary to implement technical barriers that limit the actual access to the information?

Given the broad scope of the HealthConnect system, it is unlikely that deterrence measures alone would provide sufficient control mechanisms over access to the system. It would be difficult to monitor all instances of inappropriate access – unless these came to attention via a complaint from a consumer or provider. It would also be difficult to minimise the risks associated with deliberate misuse of the system if the technical potential for widespread access exists.

On the other hand it may be impractical to implement a system with rigid and narrow technical restrictions on who has access, as such a system would not be flexible enough to support the changing needs of both individuals and organisations within the health system.

It is therefore likely that the access control policy will rely on a combination of both deterrence and technical measures to control access.

In a hospital system, there may be two levels of access control to consider. The first relating to the release of information from HealthConnect to the hospital, and the second relating to who has access to information once it is within the hospital system.

The actual authorisation to release information to a particular hospital would need to rely on a technical mechanism to allow that hospital to access the individual's HealthConnect record only when that person is admitted and has given his or her consent. To rely on policy and deterrence measures at this point, without any technical means of preventing access, would mean that all hospitals could potentially have access to the information at all times. This approach leaves the way open to risks of misuse and inappropriate access because the potential to access information is far greater than what will ever be required in practice.

Once HealthConnect information is within the hospital system, there may need to be more flexibility about which staff can access the system, and therefore access could be controlled with a combination of policy and organisational practices and some technical barriers (such as limiting which types of staff can view what information, maintaining lists of members of an individual's care team and having authentication/password processes to be followed before access is permitted).

10 Where are consent and access control mechanisms needed in the HealthConnect process?

There are four main points in the HealthConnect process where the consent and access control policy will come into play:

- At registration
- When consent settings are updated
- When an event summary is lodged with HealthConnect
- When a report is extracted or accessed from HealthConnect

These are described briefly here by way of background to the proposed consent models presented in the next section.

The other point where consent may be needed is when information (in identified or de-identified form) is extracted from HealthConnect for any secondary uses such as research or planning activities if this has not already been obtained at one of the stages listed above.

Registration

A good registration system is the key to ensuring consumers are properly informed and that consent is clearly obtained. The information a person is told when he or she first registers for HealthConnect is critical to future understanding and expectation of the system.

The registration process therefore needs to be easy to set up, and should aim to save time and resources later on.

Some issues being considered are:

- Where and how to register. For example, options include:
 - The person's GP or at a hospital
 - A Medicare office or other government agency
 - At home (via the Internet)
- What consent needs to be obtained, including for:
 - Initial opt in to the system
 - Future access to information on the system, including who should have access to what

- Information that may be potentially sourced from other systems (for example, immunisation details obtained from the Australian Childhood Immunisation Register)
 - Information flowing from HealthConnect to other registers
 - Any secondary uses of data known at time of registration
- How to record consent. Options include:
 - Written signature on application form required
 - Electronic authorisation by individual, for example, using PIN or password, a digital signature or swipe card
 - Electronic confirmation by provider on behalf of individual, for example, by having a tick box that declares consent obtained
 - How to ensure accurate identification of the individual
 - How to provide quality and consistent information to consumers:
 - through direct discussion with a provider; and
 - via a standard information kit/brochure (with additional strategies for communication to people from non-English speaking backgrounds, literacy difficulties or with other particular needs).

3.1 Updating consent settings

An individual may update his/her consent settings at any time. Some consideration needs to be given as to who would be authorised to do this on behalf of the individual (for example, all registered users of the system when probably in the presence of the individual), and when/how individuals may do this themselves (for example via the Internet or a kiosk).

3.2 An event summary is lodged

Consent may be required when an event summary is lodged if the consent settings established at registration are not applicable to the data collected, or where the individual wishes to apply different consent settings to the data.

Possible consent settings include:

- Changes to general consent settings as to who may access the individual's HealthConnect record. This could be any providers involved in treatment and care or only some providers.

- Setting consent for that particular event – or ‘masking’ the information.

3.3 Information, or a ‘report’, is accessed from HealthConnect

The advantages of obtaining consent at the point when information is accessed from the system, include:

- information will only be accessed with the individual’s consent, and it may be possible to implement a technical mechanism such as a PIN or swipe card to limit access to only these situations;
- it will be clear to both consumers and providers when access to the system is permitted;
- as consent will determine when and what information is accessed, there would be no need for an individual or provider to identify up front who may need access to the individual’s record; and
- this approach is familiar to many consumers as it is used in other types of information systems (such as banking).

The disadvantages of this approach are:

- it is unclear how cost effective this would be and whether or not it would impact detrimentally on the workflow at the point of care;
- it may not suit all consumers as, for example, it may require a person to carry a card or remember a PIN; and
- a mechanism would be needed to permit access when the individual is not present.

11 Proposed models for a consent and access control framework

The proposed models below aim to:

- reflect the individual’s consent given as to what information may be accessed by whom;
- control access to information through a combination of policy and technical mechanisms; and
- achieve a balance between permitting flexible and ready access to the system where needed, and safeguarding the information from inappropriate use and security/privacy risks.

The models also reflect the different consent options that are available depending on what point consent is sought in the *HealthConnect* process.

The main questions each proposed model aims to address are:

- What is a person consenting to and what do they need to be told?
- When should consent be obtained?
- How should it be obtained and what controls need to be placed on access to the records?
- What rules apply to how information should be handled?

At this stage, the models presented attempt to deal primarily with seeking consent and placing access controls in the context of a consumer-provider consultation. **They do not deal substantially with how to manage access to data for secondary uses when this may be required.**

The proposed models are designed to represent possible broad solutions that could apply to *HealthConnect* if implemented on a national scale, and do not necessarily represent models that could be directly applied to a trial situation.

It is therefore suggested that in order to test the various models, the *HealthConnect* trials incorporate some of the key elements of the proposed models to test which mechanisms work best and to identify what the main issues are, rather than attempt to encompass all features of any one model. The results of the trials could then feed back into further development and discussion of the proposed models.

Testing of consent and access control models is discussed in more detail in a later section of this paper.

Both models 1 & 2 involve establishing with consumers up front what they consent to in relation to information recorded on *HealthConnect*.

Model 3 provides an alternative whereby consent is obtained at the point when information is accessed from the system.

One of the key issues that needs to be explored within the research and development phase is the use of ‘masking’ of information as a method for access control. All models proposed above include an option for information to be ‘masked’. However, this is one area where further evaluation is needed to determine whether this option is a necessary feature of the proposed models.

For example, it may not be necessary to have a facility to ‘mask’ information if testing demonstrates that the added complexity does not bring any significant benefits in terms of privacy protection or consumer uptake of the system.

The consent and access control framework includes other ways in which the individual can control what information is on the system and who may access it. For example, the minimum standards outlined earlier already state that consumers would have the option of requesting that certain information not be placed on *HealthConnect* under each model. It may be that having the option of not including information on *HealthConnect*, together with other controls, provides sufficient flexibility and privacy protection for the consumer without making it necessary

to build in a capacity to ‘mask’ information. On the other hand, some consumers may wish to have certain information recorded on HealthConnect to benefit their overall health care, but only want it included if it can be ‘masked’ and limited to certain providers.

4.1 Proposed model 1 – Consent up front to any provider involved in treatment and care of the individual

Under this model a consumer would give consent to *any* health provider involved in his/her treatment and care having access to his/her information to assist in that care.

Individuals could consent to this either when they register for HealthConnect or at a later stage if they choose to change their consent settings to this model.

Individuals’ consent settings would be stored as part of HealthConnect records and checked/confirmed each time a record is accessed.

Safeguards that may be needed to support this model include:

- Clear rules around when it is appropriate for a provider to access information. These would be based primarily around the principles in privacy legislation and draft AHMAC National Health Privacy Code ie, use and disclosure for purposes of providing a health service or other specified circumstances, and include penalties for misuse.
- Information for consumers about what information different providers would have access to and in what circumstances information may be accessed
- Capacity to ‘mask’ sensitive information - ie limit access to certain providers for particular categories of information such as sexual and mental health information
- User authentication and audit trails, with active monitoring to deter/detect inappropriate use
- Capacity to tailor ‘views’ or reports so that each type of provider only has access to the information relevant to their work needs. For example, an emergency care worker would require a different type of report to a GP in private practice.
- Some way of confirming that the individual has consented to access prior to access being permitted. This may be a technical measure ranging from: the provider ticking a box and declaring that consent has been obtained and access is required for treatment and care of the individual; to a more stringent measure such as a consumer-entered PIN that confirms the consumer’s presence.

The issue here is what degree of evidence is required to confirm that access to the information is appropriate in the circumstances? The rationale behind even a notional confirmation of consent is that the provider has to actively do something to acknowledge consent before access is permitted. Without some technical mechanism in place to limit access, the potential access to the system is likely to be too broad, and will potentially increase the risk of unauthorised access to an unacceptable level.

- Where access to information is sought and the consumer is absent, a different mechanism for confirming consent may be needed. It may also be necessary to allow individuals to nominate selected providers who they consent to accessing information when they are absent, and to limit access on this basis. This would provide the individual with a clearer understanding of who may access the record when they are not present.

4.2 Proposed model 2 – Consent up front to selected providers involved in the treatment and care of the individual

Under this model consumers would give consent to *selected* health providers involved in their treatment and care having access to their information.

Similar to Model 1, consent would be obtained when an individual first registers with HealthConnect, and updated at a later stage if requested by the individual.

The key difference is that consent is only given to certain providers to access information on an individual's record. The consent settings would be stored on the individual's record. Access to the system could then be technically limited to only those providers who appear on the individual's consent settings.

Access to providers could be given to selected:

- Individual providers, or
- Groups of providers

There are a number of options for determining the basis for groups of providers. These could be identified using one or more of the following:

- Type of health provider (eg GP, dentist, pharmacist)
- A selected organisation (eg large medical practice, hospital)
- The treating team for a particular condition (eg diabetes, mental health)
- Location of provider (eg all in a certain area)
- Role of provider, based on the type of work they do in an organisation (eg treating specialist)

Draft - For Comment

Some of these criteria are likely to be more appropriate for use in relation to HealthConnect than others. While some (such as role-based groups) may be useful to identify within an organisation to determine which staff should have access to what, it may be more difficult to apply these concepts across the HealthConnect system in a way that is meaningful to both consumers and providers. The groups where it is clear to consumers exactly what they are consenting to will be most suited to HealthConnect.

A possible variation of this model is that some organisations could establish default lists of specific providers relevant to the area and type of service they provide. This list could then be discussed with the individual and additions or exclusions made as necessary. This may be particularly useful for organisations where patients have common health needs.

Safeguards that may be needed to support this model include:

- All of dot points 1 – 7 discussed in relation to Model 1 above
- A mechanism for overriding the consent settings to permit another provider having access to the information (for example, on a one-off occasion when the person is travelling interstate, or when a person unexpectedly visits a new provider).
- A technical means of limiting access to information to those providers who appear in the individual's consent settings, and otherwise refusing access

Under Models 1 & 2, when information is accessed from the system, the provider is required to confirm that they have satisfied the condition of consent. However, what is considered an appropriate level of evidence to confirm consent may vary.

For example, if a person has selected some providers they consent to access the records (Model 2), then it may be that a low evidence, more efficient method such as a tick-box is sufficient. There would already be some technical controls limiting access to the providers selected, and this mechanism would simply be a confirmation from the provider that they are accessing the information appropriately. Deterrence features are also likely to have a stronger affect as only limited providers have access, and they would be listed in the individual's consent settings making it easier to detect misuse.

On the other hand, if a person has provided broad consent to any provider involved in his or her treatment and care having access (Model 1), then it may be that stronger evidence is needed from the provider to confirm that the individual has given consent in a particular situation.

4.3 Proposed model 3 – Real time consent to any provider at point when information accessed from system

Under this model consumers could give consent to *any* or *selected* health providers involved in their treatment and care having access to their information.

The key difference from models 1 and 2, is that consent is obtained at the point when information is accessed from the system.

Safeguards needed to support this model include:

- Dot points 1 – 5 discussed in relation to Model 1
- A technical mechanism such as a PIN or swipe card that the individual enters at the point of care to prove they allowed the provider to access their records
- A back up system to support access to the system when a consumer forgets their PIN or card, that is sufficiently secure so as not to weaken the overall protection
- A mechanism to allow access in some situations (with the individual's consent) where the individual is not present

4.4 Proposed model 4 – A combination of the above

Inevitably a combination of one or more of the above may achieve maximum coverage of the ways individual could control their information on HealthConnect.

Some of the models encompass others anyway, so the cost of implementing more than one model may not be significantly different to implementing only one in comparison to the greater flexibility and coverage this may achieve.

Further consultation and evaluation of HealthConnect trials will help highlight the features of the models that work most effectively to meet provider and consumer needs. This may also point to new or additional variations of the models described above.

4.5 Other models

- Blanket consent to all providers – One suggestion was that a person could consent to all health providers having access to their information at any time, with the rules around appropriate use of information as the main means of governing access to the system.

Draft - For Comment

While the simplicity of this model is acknowledged, the model is rejected for a number of reasons. Firstly, it fails to meet the criteria that consent is 'informed' as it is too broad to give the consumer adequate information about the potential scope of situations when their information may be accessed. It is difficult to identify or limit the exact boundaries of what they may be consenting to and therefore difficult to conclude that the consent could be informed. (This is particularly so given that *HealthConnect* encompasses so many providers and types of providers Australia-wide.) Secondly, this model fails to provide a clear basis on which to control and monitor appropriate access to the individual's records. Without some means of limiting access to situations when access is legitimate, there is a potential risk to the overall trust and integrity of the system.

Model 1 above attempts to achieve as wide a scope as may be reasonably envisaged by the consumer, without leaving access open to all providers on the system. It limits access to an extent by specifying that the provider must at least be involved in the individual's treatment and care and there should be some way of ascertaining or confirming this when information is accessed.

- Allow specific categories of information to be masked – ie mental and sexual health information
- Consent at a detailed, fine grain level – At the other end of the spectrum is the option to allow a consumer to make a choice about how they would like each piece of information about them handled. This is considered both too complex and too time consuming to administer or the system to support.

Models 1 – 4 discussed above allow the consumer to control who has access to his or her information at some level. For example, by limiting access to certain providers and by having the capacity to mask information at health event level. To attempt to code at a more fine grain level that this (for example, every data item) would be unwieldy and impractical for a system as complex as *HealthConnect*.

- Opt out approach - Participating in *HealthConnect* is voluntary. For this reason, none of the trials are based on an opt out model – that is, where all consumers are put on to the system by default, and consumers would need to choose not to be on the system.