Issues Arising from Analysis of the HealthConnect Business Architecture v1.9

Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework
Australian Research Council Discovery Grant, DP0208109 2002-05
School of Law Deakin University, School of Information Management and Systems Faculty of Information Technology and Faculty of Law Monash University, Australia

Barbara Reed
Research Associate for:
Caulfield School of Information Technology
Monash University

July 2005
Introduction

This report identifies a number of the issues that are raised from the analysis of the HealthConnect Business Architecture v 1.9. It consists of a brief description of the technical architecture of HealthConnect, followed by a discussion of a number of issues of concern.

HealthConnect is a very complex system specification that is still in development. Many areas have been flagged in the specifications for further development and resolution. However its underlying design is heavily dependent on data created in one place being codified, transmitted, sent to a nominated single place of storage, verified, linked to other existing data, duplicated to the national data store, and then managed over time (access, use, and retention). These are recordkeeping issues. The technical capacity of electronic systems to deliver such functionality, and how well that functionality is specified, needs to be considered within a framework of social, organisational and individual responsibilities.

The technical architecture

At its simplest statement, the technical architecture envisaged for the HealthConnect system is a networked, peer-to-peer system. Three major layers are defined, the national coordination layer, the Health Records System and the user layer. The individual HRS's operate as a federated system, supported by common services defined at the national level, with the entirety of an individual’s EHR being stored on only one HRS (BA v1.9 p110).

The National Coordination Layer:

The national coordination layer consists of the HealthConnect governing functions, encapsulated by three high level functions:

- Administration of HealthConnect programs;
- Management of HealthConnect participation; and
- Establishment and operation of HealthConnect infrastructure. (BA v1.9 p108.)

These functions incorporate:

- coordination of registration processes including those of both health providers and consumers,
- maintenance of the National Data Store,
- Provider and Consumer Directories, access portals for consumers and providers (HCCAS and PeHAS),
- maintenance of a national HealthConnect metadata repository,
- managing secondary access to HealthConnect records,
- monitoring and overseeing all access to HealthConnect records and
- manage complaints from both providers and consumers (BA v1.9 p 20).
This role also includes defining and maintaining standards about transmission and messaging systems (BA v1.9 p19-20).

It also encompasses a records management function, specified as process B9:

C-75 In coordinating HealthConnect records management functions (Process B9) the HealthConnect governing body must organise and enforce sound processes for records management, including coordinating the records management activities of the registration services and the HRS/AEM services to ensure the integrity of HealthConnect EHR information, consumer records and provider records and that adequate processes exist for identifying and controlled handling of exceptions, including:
(a) identity errors, merge and de-merge of EHR records;
(b) suppression of EHR information at the request of a consumer or provider;
(c) recovery and change of identity;
(d) management of data loss, and data recovery;
(e) data incompatibility between HealthConnect components;
(f) extract, amendment and inclusion of HealthConnect records as a result of statutory and legal processes; and
(g) death of consumers, and death or deregistration of providers.
(HC BA v1.9, Specification of HealthConnect Business Requirements, 2004 p21-22)

Health Records System

Health Records Systems are seen as the core component of the HealthConnect architecture. They perform the functions of EHR storage, update and access control. The functions defined for the HRS applications which comprise an HRS are:

(a) Controlling access to EHR and consumer information;
(b) Maintaining consumer details and access control lists for those consumers holding their EHR on the HRS;
(c) Processing event summary information into a consumer's EHR (including maintaining managed lists and views);
(d) Responding to (authorised) EHR information requests;
(e) Interaction with the shared HealthConnect consumer index, provider directory and metadata repository; and
(f) Keeping audit trails and access logs recording all access, outputs and changes involving consumer information held in the HRS. (BA v1.9 p110)

Further, the specifications require that:

Within 24 hours of an EHR being updated (and preferably much earlier), a copy of the updated EHR material is to be transmitted in a standard format by the responsible HRS/AEM to the National Data Store for archiving and long-term retention. Together, the EHR information held in each HRS and the National Data Store comprise the HealthConnect EHR repository. (BA v1.9 p110)

User layer

Less formalised requirements in the Business Architecture have been defined for the user layer. In the main these are incorporated into the systems and infrastructure requirements defined to be the responsibility of the National Coordinating Layer (see above). They include the access portals (consumer - HCCAS and provider – PeHAS), maintenance of indexes, establishment and maintenance of metadata standards to clearly establish the documentary form
of contributions and records within the HealthConnect system, and establishment and maintenance of relationships with clinical information system providers to enable the automatic creation and transmission of event summaries.

At present the issue of individual consumer contributions to their health records, possibly through the format of health diaries, has been deferred for future implementations, mainly due to issues of medico-legal liability (BA v1.9 p4, p 65, p135).

Jurisdiction and control - governance

Jurisdiction is a critical issue for HealthConnect. The concept of a cross organisational, cross jurisdiction electronic system raises issues of ownership, custody and responsibility of both the system and its components and the information and records held within the system. This whole issue is made more complex by the emerging personal rights to control health records by the patient or subject of the health event. HealthConnect recognises these issues as valid concerns and has done so from the commencement of the project. However, now three years into the project, resolution of the issues is no clearer.

Governance issues for large complex cross-jurisdictional electronic information systems are particularly difficult to resolve. In initial exploration and formation stages it is quite common to form seemingly ad hoc groups based upon agreements of the participants. A good example of the issues is NEHTA, described below.

NEHTA (National eHealth Transition Agency) was formed in 2004 with the brief to ‘accelerate the adoption of e-health by supporting the process of reform in the Australian health sector.’¹ It is the successor to the previously operating Clinical Information Project established under HealthConnect from 2002.

The governance arrangements are described as ‘a national team funded by contributions from all jurisdictions (Australian Government, States and Territories). The team is responsible to both Australian Health Ministers’ Advisory Council (AHMAC) and Health Ministers, with a team of five AHMAC CEOs providing ongoing oversight of its activities. An Advisory Committee of experts and jurisdictional representatives has been established to provide guidance. NEHTA has been established by all jurisdictions as the national vehicle to facilitate this cooperation. NEHTA is jointly funded and governed by all Australia jurisdictions. In January 2005, the ministers agreed to establish the new entity as a company limited by guarantee, governed by a board of directors made up of CEOs from Health Departments across Australia.

¹ From NeHTA http://www.nehta.gov.au web site accessed 28.6.05
The role of NEHTA is focused on e-health informatics standards and integrating infrastructure and includes:

- Developing standards for the exchange of clinical information
- Enabling the unique identification of patients, providers, products and services
- Enabling the secure electronic transfer of information across the health sector
- Providing shared information resources
- Increasing sectoral efficiency by facilitating reform
- Establishing enabling processes to manage change
- Adopting specifications for a national shared electronic health record

This body is clearly critical to the development of HealthConnect and is a successor to a previous HealthConnect entity, although its role is not defined strictly in reference to HealthConnect. It epitomises the concerns raised by the requirement to share funding and decision making responsibility across jurisdictional borders. However, its structure as a private company also places it outside many of the established governmental legal protections in areas where state and commonwealth governments have established norms.

Similarly other HealthConnect relationships with other entities in the Commonwealth sphere are unclear. Just what is the relationship between HealthConnect and the Health Insurance Commission, Health eSignature Authority (another company established under the Health Insurance Commission), or MediConnect? Opportunistic development to gain leverage and implementation take up through finding congruence of projects is logical, however the lack of clarity about where the responsibility lines are and which organisation does what, and for whom, is endemic in this specification. This lack of clarity fosters concern that the same lack of clarity will be taken through to issues of the data and personal information residing on specific (separate?) systems.

The Governance body to manage HealthConnect itself is unclear. To guide the next phase of implementation, a revised governance structure has been determined, consisting of:

- a revised HealthConnect Board that would comprise Australian, state and territory government representatives, organisation representatives and additional expert members to provide advice on health service delivery; and
- HealthConnect Advisory Groups – to provide expert advice to the Board on health provider or consumer concerns, beginning with a Clinical Advisory Group, an Evaluation Advisory Group and an Architecture Advisory Group.

---

2 NEHTA web site
4 Ibid p.93
This is still interim and formative and does not address the longer term governance issues. It is possible that the governance model established will follow models established as precedents by organisations working in this area such as NEHTA. The Business Architecture references the possible structures including departmental function without establishing an executive agency, a company, and executive agency, a statutory authority or an unincorporated joint venture (BA v1.9 p 108,168,172). The Legal Issues Report examines five major options at a high level:

• retaining the Governance Body as a government departmental function without establishing an executive agency;
• a company;
• an executive agency;
• a statutory authority; and
• an unincorporated joint venture.5

It recommends, with appropriate provisos, that:

Our preliminary view in this matter is that, unless there is a good reason not to do so (which may include intellectual property management reasons or the reasons why the day-to-day management should be conducted under a private sector regime), the simplest structure should be adopted, at least initially. That would be retention as a government departmental function.6

The implications for this are that the Commonwealth maintains ultimate responsibility for the conduct and coordination of the HealthConnect initiative. While the Legal Issues report does raise the question of legislation to support the functions, this recommendation makes clear that ultimately the Commonwealth is the organisation with responsibility for the governance and the implementation of governance issues. The states and territories are, in this model, not directly involved in the day to day decision making of the governance body. Initially, while this may seem counter intuitive to the collaborative nature of the undertaking, the allocation of specific ultimate responsibility with the Commonwealth provides a degree of protection that is known within the records domain – that is, that ultimately, the rules and regulations of the Commonwealth for information management and recordkeeping will be applied to HealthConnect content.

Within the HealthConnect architecture the possibility of distributing responsibility for certain services to other providers, such as Medicare outlets as registration points (BA v1.9 p115), potentially private providers, who may take up roles such as that of Approved EHR Managers (BA v1.9 p42), HealthConnect Operations Centre, involving ‘more sensitive functions’ (BA v1.9 p156) or HealthConnect Consumer Access Services (BA v1.9 p117). Such arrangements may be established licence (BA v1.9 p117) or contract and contractual obligation (BA v1.9 p111). Indeed the Legal Issues report identifies a very complex network of contracting, licensing and agreements required to support the establishment and ongoing operation of HealthConnect. Each one of these arrangements needs monitoring and management.

5 Ibid p 94
6 Ibid p94
The documentation alludes to the possibility of other bodies as the implementation of HealthConnect progresses. For example ‘it is anticipated that other advisory groups may be required. This might include a privacy and access control advisory group to provide input on issues such as establishing and monitoring privacy protocols, defining consent options and rules, approval of research requests.’ (BA v1.9 p164). It is not clear how such bodies would interact with the governing body of HealthConnect. Presumably they will be mandated by the governing body to perform particular roles. Thus the suggestion that ‘This Group could fulfil the requirements for the independent and transparent monitoring of the rule of HealthConnect in authorising and managing access to information for secondary uses’ (BA 1.9 p164) seems particularly inappropriate. A body established by and responsible to a governing organisation cannot by definition provide independent and transparent monitoring.

In and of themselves innovative ways of structuring organisations and facilitating the delivery of services is not a recordkeeping problem. Innovative means can be devised for recordkeeping too. However the concerns are:

- That with the uncertainty in the key governance architecture area, recordkeeping issues will be addressed on an ad hoc basis rather than systemically. Experience with outsourcing arrangements has proven the difficulties likely to be encountered leaving recordkeeping issues to be addressed in an ad hoc manner.

- That the tactic to re-define particular issues specifically in the cross jurisdictional area for the specific project (eg in the area of privacy the development of the National Health Privacy Code), or acknowledgements that additional policy, rules or legislation may be needed (BA v1.9 p167), while pragmatic for the specific project, runs the high risk of fragmenting coherent jurisdiction based regimes such as privacy, access rights, complaints, appeals etc.

- That such ad hoc rule setting to cover particular cases also places quite a high burden of development onto the particular project initiative.

- That the lack of clear jurisdictional lines leaves responsibility for recordkeeping concerns unclear – just whose responsibility is it to ensure that these critical issues will be addressed?

- That the complex network of legal arrangements envisaged as working as contracts, licences and agreements each have a clear recordkeeping requirement for maintenance which needs to be clearly defined and as yet, has not been addressed.

- There is scepticism fostered by three years worth of project research reports about whether any recordkeeping view is actually being considered in the HealthConnect design.

Unique health identifier

Clearly to implement a national EHR system across multiple providers and consumers located in different jurisdictions, there is a requirement for unique identification of patients and health care providers. This is needed to ensure that all event summaries are appropriately linked to the correct EHR and
appropriately despatched to the HRS which is the storage node for that consumer’s EHR. Unique identification is a prerequisite to implementing a complex database design such as HealthConnect. The specifications contain the implicit assumption that there will be such a system of unique health identification. The HealthConnect principles include the statement:

- Each consumer and their EHR information will be uniquely identified within HealthConnect by use of a single unique identifier able to be linked to any future National Health Identifier. (BA v1.9 p58)

Given the controversial nature of unique individually linked identifiers within the Australian community as evidenced by the emphatic rejection of the Australia Card proposal in the mid 1970s, this assumption needs explicit attention, rather than implicit incorporation. While it is likely that the attitudes of the Australian populace have changed considerably in the intervening 30 years since the Australia Card debate, the concerns of privacy, too, have been given greater social standing and mandate in that time.

In discussions of the HealthConnect initiative and indeed, those electronic health initiatives of individual jurisdictions, political reluctance to address this issue has been identified as a barrier7. However, the HealthConnect trials in which testing of the architecture and assumptions is being undertaken, have invoked use of the Medicare number for unique identification purposes. At the same time a significant project has been approved to update the Medicare card to make it a smart card. The Business Architecture specification clearly identifies the issue:

Proposals for the introduction of a National Health Identifier (NHI) are currently being prepared for presentation to Australian health ministers and it is expected that over the coming years, consumers will be issued with a national health identifier that will uniquely identify them for several healthcare initiatives, including HealthConnect. The national consumer identification service is expected to include a client (consumer) master index linked to the consumer-held smartcard, which is available to replace the current Medicare magnetic stripe card. If approved by the ministers, and with appropriate regulatory backing, this initiative has the potential to impact on HealthConnect in the following ways:

(a) It provides a unique identifier, usable for health applications, which can be checked to avoid duplicate registration of individual consumers within HealthConnect; 
(b) It provides a unique identification token, in the form of the smartcard, on which the healthcare identifier can be stored and which can be used by the consumer to identify himself and to facilitate the access to their HealthConnect information.
(c) If developed in consultation with HealthConnect, the indexes supporting the National Health Identifier may be able to replace the HealthConnect consumer index. The entities that might provide such a service, or indeed the nature of the service itself, are matters to be determined as part of a major review to be completed by the end of 2004. (BA v1.9 p123)

As presently defined, the HealthConnect identifier seems to be considered as separate to the Medicare number, although the possibility of embedding the HealthConnect identifier on the newly devised Medicare smartcard is envisaged (BA v1.9 p114).

---

7 Discussion at the Conference 2001/2/3
Already the smart card initiative within the Medicare domain has raised concerns for privacy advocates\(^8\). This issue needs an explicit social mandate. The technique of linking desirable outcomes (such as cheaper pharmaceuticals) to consumer acceptance of the unique identifier is a technique of adoption by stealth, which may be pragmatic, but seems less than ethical given the social concern over the issues of privacy, unique identification and the capacity to build individually identifiable profiles.

This issue also exists for health care providers, although at a different level of social concern. The system similarly needs to enable unique identification of health care providers, although there is some debate as to whether it is sufficient to register at provider organisation levels or individual provider participant level. The issue is at least partially one of the granularity required for registration – should this be at an organisation level, or at an individual level. Inherent in this question is consideration of what level of granularity is required for organisational registration. The specification recognises that this is an issue – ‘HealthConnect needs to allow major organisational units (such as a hospital or clinic) to be identified separately within HC while still recognising their link to the head provider organisation’ (BA v1.9 p107). The specification also acknowledges that organisations operate in quite complex structures which are also subject to change, making management of registration quite a complex task (BA v1.9 p120). If registration is mandated at an individual level, how should this then be linked to the organisation to which the individual is attached? Such questions raise difficult technical issues of authentication, which are recognised as issues for all electronic systems.

Initially it seems that the specifications adopted a pragmatic view that registration to the level of organisation would be sufficient. The specifications clearly identify that where a provider level access is used, within that provider it will be a condition imposed upon the provider to maintain a record of those persons delegated access rights within the provider’s domain to HealthConnect (BA v1.9 p106, 120). The subsequent Legal Issues Report however recommends that this level of registration is not sufficient, recommending individual registration (Legal Issues p48) and tracking of actions at the individual level.


The Age ‘Medicare smartcard prompts privacy fears’ 21.4.2005

Or press reports on the NSW HealtheLink project, which is likely to be one of the HealthConnect HRS level systems:


Sources for registration of providers have been considered. Existing relationships between the Health Insurance Commission and individual providers in the Medicare service regime is recognised and flagged as a potential link for providing provider registration services (BA v1.9 p119). Similarly links to professional registration and licensing bodies at a state and territory level are identified as potential sources of registration information (BA v1.9 p119). While merely flagged as potential sources of registration information at this point and clearly noted that any use of such related systems would need to be the subject of explicit agreement, there are privacy issues of relevance to provider organisations and individuals inherent in such linkages.

**Privacy issues**

While not a primary focus of this report, the privacy concerns relating to HealthConnect are legion. The issues are rendered more complex with a mismatched set of privacy legislation across jurisdictional boundaries. The aim of HealthConnect is to establish a service that will ‘operate seamlessly and consistently across Australia, with the same rules for privacy, registration and consent applying everywhere’ (BA v1.9 p24).

An initiative to establish a National Health Privacy Code by the Australian Health Ministers’ Advisory Council (AHMAC) in 2003 has yet to produce an agreed outcome. A submission by principal researchers with this project advocated a higher degree of privacy regulation to manage implications of shared electronic health records, such as those envisaged by HealthConnect, as opposed to a more generic definition of electronic health records. Similarly a number of inconsistencies in the draft code were identified\(^9\). There has been no indication of whether such recommendations have been acted upon. The Draft Code has not been issued. The HealthConnect Business Architecture specification indicates the intention to use the National Health Privacy Code when it is implemented but until that time to maintain a set of tailored arrangements to meet the privacy requirements of individual jurisdictions (BA v1.9 p78). The Legal Issues Report has indicated that even with the acceptance of the National Health Privacy Code, supplementary legislation to cover privacy requirements in HealthConnect may be needed\(^10\), particularly in relation to information given about other people (relatives, sexual partners etc), genetic information, or information that aggregates in relation to particular ethnic groups (particularly Aboriginal and Torres Strait Islander people). This, then, adds further complexity to the already fragmented privacy regimes in Australia.

**Consent processes**

Participant consent to HealthConnect provisions is a complex legal area, addressed by other aspects of this research process\(^11\). Rather than dealing

---


\(^10\) Clayton Utz, Legal issues report ibid, Chapter 6, Privacy and Consent

\(^11\) See particularly the research reports and papers by Bernadette McSherry
with the full complexity of the consent process, the issues raised here are
those specifically relevant to the Business Specifications and the apparent
assumptions built into the technical specifications. Issues of consent are
intimately bound to issues of access control, and the initial access control list
(a separate process) is established at the time of initial consent.

Early discussions of consent found in the research reports and discussion
papers supporting the development of HealthConnect\(^\text{12}\) advocated a complex
and layered notion of consent whereby control of access to data held in the
event summaries could be restricted by type of event and type of provider (eg
podiatrists might be restricted from seeing sexual health reports). Such a
layered approach to access is difficult to implement and to control, both by
technology and by the health consumer. Technical constraints and ease of
technical implementation seem to have influenced the management of
consent and access in the Business Specifications. The experience of the
HealthConnect trials, too, have seemingly formalised consent models for
initial registration. A much simpler one dimensional model is now proposed
for initial adoption, deferring the complexity until subsequent post
implementation development (BA v1.9 p32).

Of particular concern in the Business Specification in relation to consent are
the following:

- That initial consumer consent includes a blanket acceptance of
  inclusion of secondary uses of the information contained in
  HealthConnect records and that this does not seem to expire even
  should a participant revoke participation (BA v1.9 p53, 95).
- That access control lists containing statements of consent as to what
  users are able to access the HealthConnect records are issued without
  time limitations, valid until a consumer changes them. (BA v1.9 p56)
- That access control lists will operate, at least partially, to the level of
  the health care provider organisation, leaving a large area of potential
  exposure to inappropriate disclosure of personal information. (BA v1.9
  p106)
- Unresolved issues relating to consent by minors and mechanisms to
  revoke or change these consents when a child reaches maturity (BA
  v1.9 p54)
- That consent to submit an event summary to the HRS should be
  explicitly given each time a practitioner sees a patient, rather than rely
  on a blanket generic consent to contribute records (BA v1.9 p31).
- That a record of all incidents of overriding of consent (for example in
  the case of emergency access, provided for in the Specifications)
  should be made and maintained.

\(^{12}\) HealthConnect ‘Consent and Electronic Health Records. A discussion paper’ July 2002
And HealthConnect Research Report 5 ‘What will be necessary to manage privacy?’ 2003
Complaints processes

In the HealthConnect architecture the responsibility for managing the complaints process is allocated to the National Coordination Layer. However the issue of different jurisdictions with different processes for managing complaints processes, both in relation to health matters and more generally in administrative matters, is acknowledged (BA v1.9 p55). The specification indicates the intent to refer any such complaints to the ‘relevant jurisdictional HealthCare Complaints Commission’, while raising the possibility of a Memorandum of Understanding to enable the Health Care Complaints Commissions to investigate complaints in private and public sector organisations (BA v1.9 p55). At this stage, it seems that complaints will be adjudicated by a body which is determined by the jurisdiction in which the event providing the subject of the complaint took place. Thus the potential for different rules leading to different determinations exist.

Recordkeeping Concerns - General

HealthConnect is clearly marketing itself as a records system. Justification for the project initiative clearly state requirements to replace or improve on the limitations of paper based records systems. Yet the understanding and views reflected in the HealthConnect documentation to date are lacking from a recordkeeping perspective. The project is determinedly focussed on a data view and information system view.

The focus of the research reports and system documentation is on the EHR itself. However, the EHR is actually a conceptual entity, rather than a physical entity. It is cumulative, exists in a number of places, contains connections to data held separately such as access control lists, and views predetermined according to defined templates, indexes, access and audit logs. Each of these separate components has different processes that dictate their incorporation into the consolidated virtual EHR. To adequately protect authenticity, integrity and reliability of the EHR, each of these processes need to be considered from a recordkeeping perspective. Attempting to address recordkeeping issues (such as retention and disposal, or access) from a single, monolithic view of the EHR is not appropriate to the project design, the conceptual models or recordkeeping as advocated by best practice industry standards.

Records exist at all layers in the HealthConnect architecture13. At minimum this entails records maintained at the National Coordination layer, the Health Record System layer (HRS) and the User layer (both individual clinical information systems operated by independent providers and the individual consumer level). While understanding the desire to sidestep the concept of ownership in favour of a more delineated assessment of roles and

---

responsibilities, this none the less has the capacity to avoid some serious recordkeeping issues. For example, paper forms such as contracts, licences, agreements and signed authorities are scattered throughout the processes to manage and regulate relationships of consumers, providers, HRS’s etc. While it assumed that the system that manages the registration processes is an electronic system under the control and custody (and ownership?) of the National Coordinating Layer, the physical evidence still explicit in the process is likely to be distributed widely amongst networks of private third party service providers. Similarly, the whole suite of administrative recordkeeping that is involved in HealthConnect at its various layers is not addressed at all, and made more complex by the lack of clarity about the structure which will be used to manage the governing body (BA v1.9 p 108).

Recordkeeping processes: registration

Registration is a key recordkeeping process. This is an essential prerequisite to enabling the ongoing management of discrete and uniquely identifiable information captured in business processes. Similarly, registration is a critical core component for the HealthConnect processes. As discussed above, each agent entity (consumer, provider) needs to be uniquely identified and associated with appropriate rights and permissions prior to being able to use or operate within the system. We would anticipate a great deal of congruence between the processes described in HealthConnect and the underlying recordkeeping processes of registration.

The issues associated with identification and registration of individuals and providers are dealt with in the specification in some depth (Processes C and D in the Business Architecture Specification). The issues of duplicate identities, pseudonyms, aliases and the rights of an individual to hide their identity yet still be able to access health services are well defined issues within the medical records sphere. Within the HealthConnect system, registration of consumers and providers is a responsibility of the National Coordinating Layer. However, it is anticipated that the responsibility will be delegated in practice to a network of consumer registration agents (perhaps Medicare and Health Insurance Commission offices BA v1.9 p115).

The design and delegation of distributed responsibility for registration will be maintained by the National Coordination Layer, presumably supported by a raft of agreements and contractual arrangements – at the administrative layer of HealthConnect which is unspecified in relation to recordkeeping, but which we can presume to live at the Commonwealth layer of responsibility. (See above, and Legal Issues report p94). The specification and development of the Consumer Registration System and Consumer Index (CRSCI) is a responsibility of the National Coordination Layer. Similarly, an individual registering as a consumer in HealthConnect must assent to the registration process. While online registration is envisioned, the process defined still mandates physical requirement of paper applications (BA v1.9 p25). The registration process itself needs to be documented. It involves authentication of documents suitable to assert identity, linkage to other systems (such as Medicare, other registries or from nominated health providers etc BA v1.9
p26) to obtain information to be included in the initial health profile and authorisation of aliases or surrogates.

The initial individual health profile, a core component of the registration process, is regarded as an initial event summary. It is anticipated that this will follow a predefined format, established in templates which can then be subjected to automatic validation for completeness. The documentary form of such templates are being developed by the Clinical Information Project (now incorporated into the NEHTA mandate).

The initial registration process also involves establishment of the initial access control list, nominating providers authorised to access the record (to the organisation level only BA v1.9 p25). The process also involves transmission of messages to the nominated providers alerting them to their ability to access the records (BA v1.9 p25). The message itself must be regarded as a record and maintained and managed.

Only after the process is complete and registration established is the consumer notified of the successful outcome, which involves the confirmation of registration, issue of online authorisations (PIN), issue of instructions on how to use and manage HealthConnect records and how to receive assistance (BA v1.9 p26-7). The issuing of such confirmation itself needs a record.

The completion of the registration process also triggers the inclusion of the entry into the HealthConnect Consumer Index (HCCI) (an action which needs to have a record associated with it). It also involves allocation of the consumer to a specific HRS, the home HRS, to which all event summaries will be forwarded for storage, following the principle that all event summaries for an individual will be located on only one HRS. The HCCI also performs other ongoing actions discussed below, which are independent of a registration process. Transmission of the initial event summary to the HCCI should also trigger the creation of a record. Given the fact that individual HRS’ will be established according to a variety of parameters (it is anticipated that there will be no more than 10, and at least initially, these seem to equate to state or regionally based electronic health initiatives), each HRS may well act according to different jurisdictional rules. Will a consumer be able to nominate or indicate a preference over which jurisdiction they choose to be associated with?

Similar processes and concerns arise from the Provider Registration System and Provider Index. One of the issues here is the granularity of registration. Provider organisations must be registered, and it is acknowledged that individual structures and local practices are different in relation to determining what the boundaries of an organisation are (BA v1.9 p74). Provider organisations are authorised for access. However individual providers also need to be registered in the system, and all event summaries need to be sourced to an individual provider, not simply to an organisation, thus associating responsibility with an individual not an organisation (BA v1.9 p36). There are unresolved issues here in relation to consistency of what
constitutes the boundaries of an organisation which HealthConnect cannot and does not attempt to resolve, rather accepting that this will be locally determined (BA v1.9 p74).

The process of provider registration is anticipated to be delegated to provider registration services, with the development and operation of the Provider Registration System and Provider Directory. The process similarly commences with an application (not necessarily in paper form, but requiring to be maintained as a record BA v1.9 p38). A validation of submitted details is performed, and a record of such checks is to be maintained in the provider registration system (BA v1.9 p39). Template proformas are anticipated to be established to manage the collection of standardised information. The completion of the registration process creates a notification to the individual provider of their registration, access mechanisms, rights etc (a record is required). The completion of the registration triggers the inclusion of the provider details in the Provider Directory and obtaining consent to publish the information from the individual provider (record required) (BA v1.9 p119).

Registering provider organisations requires an implicit recordkeeping undertaking at the provider end in addition to the generic processes identified above. These should be specified very clearly in the formal agreement to participate (BA v1.9 p41) and include security of systems (BA v1.9 p43, 45, 86, 87), obligations for training and capacity to manage internal communications and actions of their employees (BA v1.9 p167). The recordkeeping responsibilities should be very clearly identified and established in any such agreements developed, including the ‘ownership’ of records created or maintained in pursuance to such agreements. It is not clear that these arrangements are being thought of in recordkeeping terms in the documentation specifications to date.

Underlying these registration processes are recordkeeping concerns:

- That responsibility for the agreements, in whatever form these take, are specified and maintained as a record for the National Coordination Layer, rather than being left in a myriad of registration service agents.
- That the system design for the registration systems and indexes define the records needed to document the registration processes themselves.
- That messages, transmissions and moving of data from different systems (eg source data from external systems, incorporation into directory systems, and forwarding for incorporation into HRS etc) each are considered as records in their own right.

**Event summary record capture**

HealthConnect is predicated on the creation of event summaries directly following every incidence of patient interaction with the health system (BA v1.9 p33). Long term, the intention is to create automatic interfaces with clinical information systems that are capable of preparing event summaries automatically using the event summary templates being defined by the Clinical Information Project (now NEHTA). Such interfaces will be subjected
to HealthConnect testing to ensure they meet established HealthConnect standards, including those to meet security provisions (BA v1.9 p35). In the short term, web based portals to submit event summaries are anticipated. The event summaries are new records, different to and not intended to replace the individual medical records created and maintained by health providers.

Submitting an event summary, or parts of the event summary, is at the discretion of the patient (BA v1.9 p31). This raises the question of recording of consent to submit. Will it be sufficient to have an implicit consent, or should this be recorded? Each event summary submitted will be associated with an individual provider, although submitted through an organisation to maintain clinical responsibility (BA v1.9 p74).

Practitioner concerns have included the degree to which the event summary can be regarded as complete, given the discretionary nature of submission. The issues of liability in acting or not acting on the information contained within the system is of concern (BA v1.9 p55). The Legal Issues Report identifies a number of practical mitigation strategies, including clear education and training of practitioners in understanding the limitations of the system, and establishing norms of practice by peer professionals to guide appropriate usage.14

There are issues of uptake and critical mass. Until a significant number of providers and consumers are using the system, the value of the information recorded is in doubt (BA v1.9 p54).

Transmission of the event summaries is partly a function of the nature of the interface technology in place. While clinical information systems in the longer term may be capable of instantaneous extraction, translation into the HealthConnect templates, and submission to HealthConnect as one seamless process, this is not yet the reality. In the interim, issues such as manual completion through web portals or work around batch submissions may be implemented. In reality, the likelihood of practitioner uptake is inhibited by adding extra steps to clinical practice.

The transmission process will act via the HealthConnect Consumer Index (HCCI) whose role it is to provide the linkage information needed by the messaging and transport protocols to identify the appropriate HRS on which the consumer’s EHR is stored (BA v1.9 p116). Thus the HCCI must maintain records on routing and transmission to enable tracking of the process of submission.

Individual providers may maintain a copy of the event summary they submit to the HealthConnect system, although this is at their discretion. This issue has been subject to comment to HealthConnect and the extent to which it is an issue for individual providers is referenced in the Legal Issues Report, which

14 Legal Issues report, Chapter 8, Liability and Indemnity.
specifically states that guidelines on appropriate use of HealthConnect should address:
What records the provider (and the HealthConnect system) should keep of what views of the HealthConnect record were accessed by the provider in a session (this is relevant evidence as to what the provider viewed and may have used to make a clinical decision).\textsuperscript{15}

**Definition of templates, data formats**

Event summaries undertake different purposes, from initial registration creating a health profile, to records of consultations, to emergency service provision, etc. The requirement for uniformity of information gathered is well established within the HealthConnect business specifications. The Clinical Information Project was the initial body tasked with defining the format and content of the event summaries. This was to be done in close consultation with the practitioner community. This project has now been subsumed into the NEHTA organisation, confusingly separate to the HealthConnect project, when one is so much dependent on the outcomes of the other.

However, the requirements for specific and standard forms, expressed in the form of XML metadata templates or incorporated into schema definitions or stylesheets, have been identified as critical infrastructure in all electronic health processes. The confusing and continually evolving picture of standards issued in this area include initiatives of the HL7 transport and messaging protocols, CEN EN13606 reference model, the research initiatives of GEHR, archetypes etc, all recognise the importance of standardised definition and expression of data elements constituting the health record. HealthConnect has been distanced from the definition of the health ‘infostructure’ with the creation of NEHTA, however they are critical stakeholders in the process.

The area of defining metadata templates to accord with the data elements defined to support specific record types is one area where HealthConnect has appropriately identified recordkeeping issues (although these are not expressed as recordkeeping issues). The definition of the HealthConnect metadata repository is a confusing expression, but taken to mean the repository of the metadata template definitions that will support the HealthConnect implementations (BA v1.9 p123-4). A more accepted term for this functionality is the emerging concept of a specific industry/implementation metadata registry.

The specifications recognise that templates will change over time (BA v1.9 p156). It identifies that each EHR event summary, view, list, query etc should be tagged with the metadata version of the template that created it (BA v1.9 p144-5). It recognises that each version of the templates will need to be maintained in the long term, to enable continuing accessibility and meaning to be attributed to records submitted according to superseded templates (BA v1.9 p144-5, 156). Similarly the requirement will be to maintain cumulative records of changes to encoding schemes used to derive data values (eg

\textsuperscript{15} Legal Issues Report p 84
SNOMED classifications etc) (BA v1.9 p126). This, too is a recordkeeping issue.

**Duplication of information**

The roles and responsibilities for the various technical layers of HealthConnect seem apparently independent. However, there are large areas of duplication of information across different data stores as defined in the specifications.

For example, the HCCI, the consumer Index, is a system of the National Coordination Layer primarily responsible for enabling transmission of the individual event summary to the appropriate HRS on which the individual's EHR is stored. This index is distributed (or made available) to the registration agents and data is sourced from the registration process. However, it is also clear that this whole system is duplicated with a master copy being maintained by or on behalf of the governing body. This master copy will hold more information than the generally available index and it is the master copy which will be used to re-establish consumer identity in the event of loss (BA v2.9 p116). Update or alteration of consumer registration information is done through the EHR, held at an HRS layer. This information is copied to the HealthConnect Consumer Index held by registration agents (and presumably to the master copy)(BA v1.9 p140).

Similarly, the HRS is determined to be the authoritative source for all of a consumer’s EHR, however there is a requirement on HRS to transmit copies of all event summaries to the National Data Store, within 24 hours of an EHR being updated (BA v1.9 p110). Confusingly the requirements state ‘Information held in the NDS will replicate information contained in, and received from, each HRS/AEM as EHR extracts rather than being a reconstruction of the EHR from basic transactions’ (BA v1.9 p131). We understand this to mean that the HRS sends a particular view of the EHR data to the NDS, rather than sending the event summaries themselves, but it is not clear. Access logs maintained by the HRS’ are similarly sent to the National Data Store for long term storage and retention (BA v1.9 p155).

The issues raised in these areas of duplication are:

- Which data stores contain records to be regarded as the primary, original, complete and authentic record?
- If it is to be the record in the National Data Store (a logical assumption as this is the version maintained for archiving and long term storage purposes), this means that the health records in this system will be defacto commonwealth records, not state based records, regardless of the jurisdiction controlling individual HRS’.
- Issues of synchronisation of multiple data stores containing variations or versions of the same information will need careful management.
- Records are needed to ensure that verification of transmissions, synchronisation exist.
• Will the roles and responsibilities associated with the different layers and different copies of the same data be clearly identified and delineated?
• Will different jurisdictional rules determine that different treatment of records in different stores or systems are applicable?

Storage in HRS

The individual HRS’ are held to be the core components of the HealthConnect system. Individual event summaries are routed to the nominated HRS through the HealthConnect Consumer Index. Event summaries will be authored by a variety of health providers, each individually attributed, involved in an individual consumer’s health care over the period of a lifetime. Each event summary must be numbered in some unique way by the receiving HRS, as well as containing the consumer’s HealthConnect unique health identifier. The former is required to manage the event summaries as records and independent entities able to be linked. The latter is required to enable individual event summaries to be linked to the cumulating EHR relevant to an individual.

Access to information on an individual’s EHR will not be through individual event summaries. Rather it will be through filtered views known as EHR views and lists. Views are generic presentations of the data in event summaries (‘redefined set of data items selected from an EHR, processed and returned in response to an EHR request’ BA v1.9 p135). Lists are ‘a special form of the more general EHR View and carries with it some notion of persistence, completeness, currency, maintenance and/or order’ (BA v1.9 p136). Lists are either ‘derived lists’ or ‘maintained lists’. Derived lists are ‘those that can be automatically generated by querying all relevant event summaries. A derived list is the EHR view that results by running a predefined query against a consumer’s EHR information in accordance with parameters supplied as part of the query.’ (BA v1.9 p135). A maintained list is ‘an EHR list maintained by a process of review and update by providers having knowledge of the consumer’s condition and treatment’ (BA v1.9 p 137) for example, Current Medications, Active Problems/Diagnoses, Adverse reactions etc.

These views and lists are created according to templates (again defined and promulgated by the Clinical Information Project – now NEHTA) and care is being taken to ensure that compiling views/lists will ensure the integrity of the information presented and that all relevant components of the EHR are always included so that information cannot be misinterpreted or seen out of context (BA v1.9 p44, p 136). While not mandated, it is suggested that these derived lists are dynamically generated as the event summaries are received, thus information is stored in HRS according to views, rather than generated dynamically when requested (BA v1.9 p136).

Lists or views that are generated automatically and stored within the HRS are records in their own right and will need to be managed as such – they will need versions, dates etc. A preliminary indication that this issue is
appreciated is included in the specifications (BA v1.9 p137). Similarly every query run against an individual’s set of event summaries will produce a customised view or list. These, too, will need to be regarded as records and stored, uniquely identified, versioned and dated in addition to the message or query that evoked them, records of the process that was undertaken to generate them, and transmission details of who they were sent to and when.

Storing event summaries will be logical rather than physical. There is no such thing as ‘the EHR’. It consists of component parts stored separately, linked (persistently?) through a variety of mechanisms, the key one being the unique health identifier. This reinforces the importance of taking a process oriented view of recordkeeping, which identifies and manages the mechanisms of production as well as the outcomes. This view diverges from the more simplistic management of outputs, or records as objects.

**Access**

Access is the process most completely defined in the HealthConnect documentation, as it is an overwhelming concern when managing sensitive personally identifiable information.

Consumers have rights to control access, reflecting a changing attitude to the ownership, custody and responsibilities associated with managing personally identifiable information. With the integration of user contributions to their own records, questions of shared responsibilities for records creation and management are opened up. As yet these areas are vague and undefined, but they indicate a significant departure from the organisation or provider centric view of records that is common in most contexts, and will have significant impacts on the management of recordkeeping rights and responsibilities over time.

The initial registration as an individual within HealthConnect includes a process for establishing an initial access control list, a list which details which providers (at an organisational level) may access the information stored within the HealthConnect system about the individual. As a part of the registration process those nominated providers are potentially contacted to contribute information which will assist in compiling the initial health profile compiled at the registration process (BA v1.9 p 25) and will be notified of the access rights granted to them. As indicated above there is an issue to be addressed about the granularity of access being provided. HealthConnect is only intending to control access to the layer of the organisation. Within the organisation policies and procedures will need to be defined to ensure that unauthorised and inappropriate access is not permitted (BA v1.9 p107,120)\(^{16}\). This leaves the consumer vulnerable to the procedures of individual organisations, particularly if the HealthConnect record is brought into the organisation’s own

\(^{16}\) See also, ‘consumers will not be able, through HealthConnect to deny access to an individual provider within an authorized provider organization, though it may be possible for the consumer to address this requirement with the relevant provider organization’ BA v1.9 p56
records system, as is anticipated. Similarly, the complexity of masking or filtering the views for specific types of providers has been removed from this version of the HealthConnect specification, while significantly present in the previous version of the specifications (v0.9), presumably due to technology barriers (BA v1.9 p32).

Access control lists are within the active management of consumers. It is anticipated that the consumer will monitor and alter the access control lists using the HealthConnect Consumer Access System (HCCAS). Other functionality envisaged for the HCCAS includes maintenance of registration data (demographic etc), accessing individual event summaries and views compiled from the consolidated event summaries, accessing audit trails to check who has accessed their records, and, in the future, contributing end user event summaries in the form of health diaries, comments or reporting of results (BA v1.9 p64, 65). It is not clear from the specifications how the HCCAS will work. At present it is defined as a web based portal, which presumably interacts with individual HRS (BA spec v1.9 C56, p13), through the routing mechanism inherent in the Consumer Index. Queries, updates and contributions to the event summaries, lists, views and access audit trails will all need to be maintained as individual records, sent from the HCCAS to the relevant HRS.

Access control lists, then, are maintained as a separate record, within the HRS and possibly the Registration system. Again, at this stage it is not clear from the specifications; however the potential for duplication of the information further raises the issue of synchronisation and accuracy referred to above. Access control lists will be able to be updated and amended by consumers. The requirement will be to maintain the access control lists as a record, with clear indications of the authorities that existed at a nominated period (ie not to be regarded as a data source which can be continuously updated with no cumulative record).

Obvious concerns over access to sensitive personal information have driven the requirement to maintain an externally queryable audit trail associated with all access to the EHR. This audit trail is associated with the individual EHR (presumably meaning the cumulative resource consisting of event summaries, views, lists and access control lists linked to a single unique identifier) providing a record of all (successful?) accesses to the specific material linked to the unique health identifier. This audit trail, linked to the specific material within an HRS relating to an individual seems to be the recordkeeping trail anticipated in the HealthConnect system design. Unfortunately expressed as an audit trail, this would, from a recordkeeping perspective, be better expressed as a transaction log. While the emphasis on being able to query transactions relating to access reflects the overwhelming public concern on access, equally all transactions relating to the cumulative record needs to be logged in a similar manner to meet appropriate recordkeeping concerns. Some of this notion is already incorporated specific application specifications, as indicated in the specification comment ‘the registration applications are to log all transactions as an audit trail, which is to be archived indefinitely’ (BA v1.9 p156).
The access log is to be archived to the National Data Store\textsuperscript{17}. Similarly, the National Data Store itself is to maintain an access audit log (BA v1.9 p113). It is not clear whether these two records, which should exist independently, will actually be consolidated into one log at the National Data Store level (‘a consolidated access log is also to be maintained as part of the national data store data collections’ BA v1.9 p157). Being able to interpret the access logs over time will require similarly robust links to time bound Provider Directory records, maintained to enable interpretation of who has accessed the specific records.

**Updating and correcting information**

The activities involved in the HCCAS application specification include a consumer being able to update information relating to their profile, access controls and, in time, to be able to contribute event summaries. All these types of interaction involve direct communications between the HCCAS and the HRS. In addition, the HealthConnect specification identifies a mechanism through the HCCAS whereby a consumer can seek to correct factual information. The rules guiding how this will work have yet to be fully defined (BA v1.9 p55), but it envisages that a correction may be made or a comment may be added to an event summary to reflect the desired change. As noted elsewhere\textsuperscript{18} this is a matter covered in Freedom of Information legislation, which exists at both Commonwealth and all state and territory levels. Details on the mechanisms allowed under the various legislation are different, with some legislation enabling expunging of incorrect material and others enabling comment provisions. Reconciliation of these differences will need to be met in the HealthConnect specifications for correction of information.

HealthConnect clearly follows the general norm, in providing that any corrected information will not be deleted, but will be used in preference to the older information which will be masked from view (BA v1.9 p33).

**Use**

Use of HealthConnect EHR’s and their representations as views or lists is not discussed in the specifications as a process separate to that of access, with the exception of secondary use (discussed below). Essentially HealthConnect as specified at present is a passive system. It accepts event summaries produced by clinical information systems maintained by individual health providers. It enables access to and extraction of information from EHRs by health providers. Initial discussions on providing decision support systems to enhance the use of the information in the system are now not considered a part of the initial implementation of HealthConnect (BA v1.9 p57, 75) and are left to third parties to develop. Some limited ‘user notifications’ are considered part of the initial implementation (BA v1.9 p51, 55) but this aspect in the

\textsuperscript{17} ‘HRS is to regularly forward copies of EHR information and logs of audit trail accesses to the HealthConnect Data Store for archival storage and approved secondary uses’ BA v1.9 p155

\textsuperscript{18} Iacovino and Paterson op cit
current specification has been considerably reduced in importance from earlier versions.

How information stored in EHR’s is used by authorised providers is still very unclear. It resides with the individual clinician or provider organisation. At present the arrangements with health provider organisations outlined indicate that agreements with providers will need to include statements of appropriate use of information sourced from HealthConnect (BA v1.9 p119), particularly in line with privacy principles. However, requirements for safeguards against misuse of information are identified as one of the governance issues that will need to be addressed (BA v1.9 p167). The Legal Issues Report further identifies limitations on use under existing copyright legislation.

For the health practitioner these issues are substantially more important than they are for the development of an information system to support the passive storage and access mechanisms. For practitioners the practical implications of having a system such as HealthConnect raises considerable issues in terms of their requirement to access and use the information contained in the EHR’s as part of their clinical decision making. Access to the information is filtered through ‘views’ (discussed above), rather than directly through access to each event summary. Use of the information is left to the discretion of clinical decision making processes. For the practitioner they impact on the expectations and quality of services provided, impinging onto professional liability issues. If the information is available through the system, can they rely on it, are they required to use it?

The Legal Issues Report investigates this aspect of professional liability in more detail. The Legal Issues Report states that there are no new liability issues involved with the promulgation of HealthConnect, that the liabilities are generically already present in clinical practice. However the extent to which liability will be attributed will depend on ‘reasonable clinical practice’, which in the context of HealthConnect has yet to be determined (Legal Issues p 79). This is an area in which the Legal Issues Report recommends the establishment of a peer standards groups in ‘designing HealthConnect templates and views and in setting sensible guidelines for use of HealthConnect in clinical practice’ to determine that such risks are acceptable to practitioners (Legal Issues p79). Similarly the report recommends that clear guidance is continuously available to clinicians on the limitations of the system, while also recommending that care is taken to define and perhaps limit liability for those operating the actual electronic systems.

For clinicians, the issue is also one of uptake. If the information provided in HealthConnect is partial and covers a minority of their patients, how much value is derived from their participation? HealthConnect acknowledges the issue of managing both provider and consumer uptake as issues, with an implementation strategy for consumers focussing on identifying priority target groups with health problems or profiles likely to gain immediate benefit in take up of the system and an acknowledgement that almost all the functions envisaged for HealthConnect need to be in place for provider uptake to be successful (BA v1.9 section 13.1.2 Provider and Consumer Take Up). One of
the worrying aspects of the strategy to achieve provider participation is the linking of other, perhaps more desirable, functionality with the need to register with HealthConnect as a provider. In particular this is clear in the inclusion of use of the e-health message bank services. The ehealth message bank service is a new aspect of implementation introduced in this version of the system specification. It is intended to ‘provide facilities needed to receive, hold and forward eHealth messages being transmitted between participating providers for purposes such as electronic prescriptions, electronic referrals, electronic notifications and, potentially, a range of other health-to-health (H2H) and B2B transactions.’ (BA v1.9 p147). This service is required as an infrastructure layer to manage communication and transport between the various layers and technical components of the HealthConnect information architecture, but it is seen as a separate application with greater application than that of HealthConnect alone (BA v1.9 p 3). Yet to use this service, registration within HealthConnect as a provider would be necessary, regardless of whether the other aspects of HealthConnect functionality are used by the provider (BA v1.9 p81-82). This adoption of an implementation strategy which deliberately mixes functionality, involves sign up for multiple applications, or even sign up by default, grates. It may be an effective means of ensuring greater participation within a limited time period, but it is inherently deceptive.

Secondary use

Secondary use is a function managed by the National Data Store level within the HealthConnect architecture. It is directly and solely under the control of the HealthConnect governing body. It is a component which causes considerable public concern for privacy advocates, particularly comprising such sensitive information and has, as such, received considerable attention in the specifications of HealthConnect.

Use of the information within HealthConnect for a variety of reasons that do not relate to the primary provision of health services to an individual, is long accepted. Within the HealthConnect specifications, the reasons listed are ‘research and planning of health service delivery’ (BA v1.9 p2) serving ‘researchers, planners and managers, evaluators’ (BA v1.9 p 3) who ‘will access data through ‘reports’ that are extracts of EHR information that have been predefined as part of the HealthConnect secondary use approval process’ using the National Data Store (BA v1.9 p7). All discussion of secondary uses is accompanied by the qualification that such use is ‘under strict privacy and ethical protocols, appropriate legislative requirements and monitoring of such use’ (eg BA v1.9 p38).

Secondary use is generally anticipated as being access to ‘aggregated or de-identified’ data from the HealthConnect system (BA v1.9 p46) through predefined reports which are constructed to meet the criteria established by the research project. However access to identified information is possible and shall be provided in accordance with legislative provisions outlined in the National Health and Medical Research Council Guidelines s 95 and 95A, subject to greater scrutiny and monitoring controls (BA v1.9 p46).
continuing community concern is whether deidentified information can be reconnected to its identifying details, whether this be by small cell inference (specifically noted as a concern BA v1.9 p 97) or by other means.

Some research use of identified information is permitted. Amongst those nominated is the evaluation and review of particular performances (BA v1.9 p93). The privacy and protection of provider information is not ever specified within the specification. This leads to the inevitable conclusion that the data set that comprises the HealthConnect information base in the National Data Store will be capable of much greater monitoring of particular provider services than is currently available. Health providers could legitimately see this as an increased degree of surveillance of their practice. For the health providers this should be an issue of considerable concern, particularly given the fact that this type of monitoring and any protections for providers are not specified at all.

For consumers, consent to secondary uses is now encompassed in initial consent to participate in HealthConnect (BA v1.9 p53). There is no capacity to opt out of the secondary use provisions. This bundling of permissions is an issue which has emerged through the generations of specifications, with earlier versions foreshadowing a more detailed degree of permissions for secondary use in addition to greater granularity in providing permissions for primary use of personal health information. The experience of the trials of HealthConnect seem to have resulted in this much less contextually based consent, possibly because of the difficulties of technical implementation, as discussed above. However, with a generalised consent process for secondary use, which has no limitations on period, type or whether it is for identified or de-identified information, the consumer has lost considerable control over the use of their personal information. This bundling also raises the issue of whether the overriding consent to secondary uses meets the criteria of ‘informed consent’.

The implicit requirement is for consumers to trust in the ‘transparent monitoring’ controls that the HealthConnect governance process will put in place. As discussed above, the issue of which body will be the monitoring body and how this will operate is a key issue in establishing this degree of trust. As currently being discussed, the possibility of the privacy and access control advisory group established as part of the governance structure is mooted as a possible body to provide such transparent monitoring and review processes (BA v1.9 p164). As discussed above in the governance section of this report, the lack of independence of this body should render it ineligible to perform the monitoring function. The need for an independent body, external to the HealthConnect governance structure is recognised in the statement ‘Clear lines of decision making for determining the secondary uses of HealthConnect data, including ethics approval and independent scrutiny by an expert external to the HealthConnect governance framework’. (BA v1.9 p168 identifying HealthConnect checks and balances.) There is clearly more work that needs to be done in order to finalise these arrangements.
There are issues largely unresolved about the degree to which an overriding consent process will meet the requirements of the privacy legislation. This legislation specifically provides that an individual has the right to specifically authorise use of personal information which exceeds the initial reasons for collection. The blanket consent at registration will disempower consumers to choose to participate or not to participate in research, evaluation and other uses of their potentially identifiable data. To an extent there is a possible gliding around the provisions which are designed to empower a greater individual control of use of personal information in the ellipse statement that HealthConnect serves the purposes of secondary research as one of its primary functions. Thus the collection and use of the information contained within the datasets will fall by default within the permission zone. Similarly in the legislation controlling access to health information there is an exemption for secondary uses if ‘the disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services’ (example from NSW HPP 11, Limits on disclosure of health information). This type of exemption still does not cover every instance of research use of data, whether it is deidentified or not. It also transfers a significant degree of control over use of personal and personally identified health information away from the explicit control of the consumer, onto the body responsible for assuring ‘approved secondary uses’. In the absence of a clearly defined privacy regime for HealthConnect, this important area is still undetermined. However, this type of transfer of responsibility is surely against the spirit of the privacy protections now enshrined in legislation and similarly in contrast to the encouragement of individuals to take more active role in the management of their personal health information.

As currently articulated, permission for secondary use of the personally identified information extends beyond the life of the consumer (ie beyond the capacity to give consent) (BA v1.9 p61). Similarly the data will continue to be available for use for secondary purposes after a consumer opts out or deregisters from HealthConnect participation (BA v1.9 p61). While the opt in consent includes by default permission for secondary use, the reciprocal opt out provisions do not contain the capacity to revoke permissions for secondary use of personal information.

The notion of recordkeeping supported by HealthConnect is very dependent on the EHR itself (or rather its logical component parts) being treated as the single record of note. In the process of applying for and being screened for secondary use rights, a significant number of records are created at the HealthConnect governance layer which will need management. These include applications, assessments, confidentiality or other undertakings, analysis of requirements, devising of appropriate reporting parameters across the HealthConnect data, and monitoring of usage.

The National Data Store is the locus of all processing or production of reports to support secondary uses. The National Data Store itself is subject to the requirement to keep access logs (BA v1.9 p113). It is not clear whether use of personal information.

---

of a particular EHR for secondary use purposes will write an entry to the audit log for the specific individual’s records. Nor is it clear whether a consumer can access audit logs of the National Data Store, thus available for scrutiny by the consumer – all reference to consumer access to their EHR is by impute through the HRS layer of the architecture (eg BA v1.9 p 62 and more specifically in BA v1.9 p110). While there is mention of a ‘consolidated’ access log to be maintained at the National Data Store layer (BA v1.9 p157) it is not clear whether this consolidated access log includes the access logs of the National Data Store itself, or whether these are consolidated from the registration agent and individual HRS levels. Nor is it clear how a consumer would get access to this log.

Recordkeeping as audit trails

Within the specification for HealthConnect, the recordkeeping requirements are not well established, with the emphasis being on consideration of the EHR. The inclusion of audit trails to monitor access is the key component of the recordkeeping strategy that has been articulated for the system. However as is clear from the specification, the EHR is a logical rather than a physical record and the specification clearly identifies at least 9 different components which contribute to a single EHR (BAv1.9 p129-130). Each of the components may or may not be physically in the same database and each has different means of compilation, whether that be through manual contribution, ingest or by system logging (eg in the case of version logs, access logs or audit trails).

There is some confusion about whether the access log and audit trail are the same thing. Typically the access log would be a subset of the audit trail, containing only those references to who has accessed the record, whereas an audit trail would reflect all actions undertaken on any record, including information alteration, update or system changes etc.

The content of the audit trail is detailed as ‘The audit trail report will display the name of the organisation, the user who has accessed the information and the various parts of the participant’s health records that were accessed.’ (BA v1.9 p74). Details of the anticipated contents of the access log and audit trail are included in the specification (BAv1.9 p141-142).

For recordkeeping purposes, the technique of audit trails generally is a poor recordkeeping tool, requiring complex reporting to reconstitute the events which affected the record. In the case of the HealthConnect specification, it is clear that the audit trails/logs are to be maintained linked persistently to an individual EHR by means of the unique identifier, thus providing a much more contextually grounded record. However, the audit log will potentially be physically created and stored at a number of layers within the HealthConnect architecture, including the registration layer (BA v1.9 p146) and the HRS (BA v1.9 p112). Each of these layers is instructed to dispatch the access logs to the National Data Store, which then manages a ‘consolidated’ access log (BA v1.9 p157). As indicated above there is a lack of clarity about whether the
National Data Store’s audit and access logs are incorporated into this consolidated access log and how consumer access is gained to this record.

For recordkeeping purposes, it is not enough to have a partial record only, but every instance of every transaction that takes place on a record must leave a trace which can be queried. It may be that this view of audit logs will support the notion of linking such actions to the specific record, which is the desirable recordkeeping state for EHR information, but it is not clear that this is the case. More usually audit logs are used as system tools to provide back up or recovery when required. However, all instances of all transactions (including system administration, reporting and secondary uses) conducted on any part of the EHR should generate a recordkeeping transaction. Typically such complete audit logging approaches to recordkeeping frustrate system administrators as the size of the audit trail can become prohibitive. Given that, some decision making about exactly what events should be retained indefinitely is definitely missing in the consideration of the audit trail/access log as a recordkeeping tool in HealthConnect.

This technique only addresses the data components of the EHR and as indicated throughout this report, records occur throughout the processes specified in the Business Specifications. Different means of achieving an appropriate recordkeeping outcome might be achieved if the whole system was considered from a recordkeeping perspective. Certainly the simplistic reaction that all data relating to an individual EHR will be maintained indefinitely is one which should be subject to considerable future scrutiny, as discussed below.

**Disposal, retention**

Retention and disposal of personal information is a vexed issue, typically managed through archival legislation although over the past few decades this has been made more complex with the introduction of general privacy and health specific privacy legislation mandating destruction of personal information once the purposes for which it was collected have passed.

HealthConnect is clearly establishing its position as a maintainer of the archival record. The specifications clearly state that ‘The EHR data will be permanently recorded and preserved subject to legal constraints’ (BA v1.9 p34), raising once again the issue of governance and establishing which legislation will be appropriate to control such long term preservation. By default, pending resolution of the governance issues, if the archival responsibility exists at national level, it will be Commonwealth legislation. However, each of the HRS and contributing provider will be located in many jurisdictions and subject to the retention rules of that jurisdiction. This creates a potential anomaly whereby information may be deleted in the creating environment, only to be legitimately retained or destroyed at different times in a different jurisdiction. This, apart from confusing practice will cause significant potential synchronicity problems between the various databases and also anomalies of access.
The HealthConnect data resides in many component applications as identified through this report. The requirement for indefinite long term retention (beyond the life of a person) means that the information within the records must be accessible. Thus recordkeeping must be a component of each of the key applications that contribute to the consolidated logical EHR. This includes the registration data bases, the provider directories, and the metadata repository containing the template specifications. The challenges of maintaining accessibility of the information is under presented in the specification.

At the same time as the specifications imply complex long term retention requirements there is a simplistic notion of everything retained indefinitely. As discussed through this report, there are records supporting transactions throughout the specifications. Not everything needs to be retained for ever. There are privacy concerns about aspects of these simplistic requirements, particularly in the notion of maintaining an indefinitely retained record for people who have opted out or deregistered from the system. While medico-legal requirements can be cited for a period of retention, the indefinite retention and continued use of the information for secondary purposes seems beyond the scope of consent permission supplied at registration. Management of this aspect is only partially covered by the requirement to mask or withdraw the information from viewing (BA v1.9 p61).

**Archiving**

The National Data Store is clearly identified as the component of the HealthConnect architecture that will be responsible for the long term retention of the EHR (BA v.19 p7). This key design principle then allows individual HRS implementations to destroy records with confidence once they deem it appropriate (not withstanding the earlier comments on conflicts of jurisdictional regime). Given the replication of the record, it does not need to permanently reside in more than one place, although there is a clear requirement for managing operational accessibility to the record for as long as it is required within the HRS. There is no consideration of this within the specifications.

It is curious that the specifications contain such a prescriptive requirement to transmit copies of EHR event summaries to the National Data Store 'within 24 hours of an EHR being updated (and preferably much earlier)' (BA v1.9 p110). This may be to ensure that the National Data Store can effectively function as the disaster recovery component of the architecture, but it is not clearly identified.

The challenges of maintaining technology dependent electronic records for long periods is recognised only briefly in the statement ‘the very scale of HealthConnect represents a significant challenge to its ability to acquire, configure and manage underlying processing technologies for the long term. (BA v1.9 p127). The challenges to maintain an appropriate set of metadata templates reflecting changes over the life of the system is much more completely specified (BA v1.9 p145), encompassing emerging changes to
structures, requirements for backwards and forwards compatibility, requirements to enable time bound version controls and changes to supporting terminologies over time.