Arch Sci (2008) 8:37–68
DOI 10.1007/s10502-008-9070-1

ORIGINAL PAPER

Recordkeeping research tools in a multi-disciplinary context for cross-jurisdictional health records systems

Livia Iacovino · Barbara Reed

Published online: 26 September 2008

Abstract An Australian Research Council project, *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework*, brought together experts in recordkeeping, privacy, confidentiality, intellectual property, torts, medical law and ethics to address concerns with a major networked Australian health record initiative. The research required developing innovative research tools and understandings, which provides an exemplar for methodologies to address multiple-disciplinary concerns and priorities that set a precedent for future inter-disciplinary collaborative projects concerned with the analysis and design of such systems. This article provides an analysis of the research design, methods, tools and findings of the project which operated within a records continuum framework.

Keywords Multi-disciplinary research · Recordkeeping research methods · Health records

Introduction

> Detailed analyses of the nature of the privacy interests inherent in different types of records are urgently required to enable archivists to make more thoughtful and informed judgments about the varying degrees of sensitivity associated with specific records and the types of harm implicated in their disclosure (MacNeil 2005, p. 79).

As advocated by Heather McNeil, archival understandings of privacy in different contexts have become urgent as sensitive information, in particular health, can no longer rely on

L. Iacovino (✉)
Centre for Organisational and Social Informatics, Caulfield School of Information Technology,
Monash University, P.O. Box 197, Caulfield East, VIC 3145, Australia
e-mail: Livia.Iacovino@infotech.monash.edu.au

B. Reed
Recordkeeping Innovation, P.O. Box 1275, Darlinghurst, NSW 1300, Australia
e-mail: B.Reed@records.com.au

protection behind the walls of a trusted organisation or an archival institution. Archivists and records managers must involve themselves with other stakeholders in policy developments and business specifications for large-scale health and other electronic transaction systems which are the future of government and private enterprise business.

The issues raised by networked electronic health systems managing patient health records involve a complex interplay of law and ethics (for example, in the context of informed consent), between common law developments and statutory frameworks and between legal regulation and recordkeeping best practice (for example, a record will be of little or no evidentiary value unless it can be authenticated, and legal sanctions against fraudulent practices will be ineffective in the absence of record traceability). Archival issues include the potential absence of recordkeeping functionality, the loss of accessibility to the records during transfer to a new technology or accidental loss due to media failure affecting the integrity of the records. To be socially and ethically responsible, a national network of patient health records must be underpinned by legal guidelines to ensure legislative protection, in particular privacy; recordkeeping strategies that will engender trust in electronic health systems; and secure patient and doctor identifiers linked to authentic health records over time.

An Australian Research Council (ARC) project "Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework" brought together experts in recordkeeping, privacy, confidentiality, intellectual property, torts, medical law and ethics to explore a specific type of record—a shared electronic health record—on a wide range of legal, ethical, record and system issues from Australian and international perspectives (Iacovino et al. 2006).The design of the research project is an example of innovative collaboration across disciplines. Achieving congruence of ideas, identifying differences in approach and methodologies and building networks of excellence across the disciplines enabled cross-fertilisation and the development of new partnerships and collaborations.

Health*Connect* as an electronic health record (EHR) exemplar

In Australia, in 2000, the National Electronic Health Records Taskforce recommended the creation of Health*Connect* as a joint health ministers' project to oversee a nationally coordinated and distributed network of electronic health records (EHRs) (National Electronic Health Records Taskforce 2000). Health*Connect* as a term was applied to the proposed national health information network and the project itself. These two aspects of Health*Connect*—the network or system and the project to develop the network—are evident in the early statements of their purpose:

> Health*Connect* is the proposed national health information network to facilitate the safe collection, storage and exchange of consumer health information between authorized health care providers (Health*Connect* 2002b, p. 3).

> The Health*Connect* Project is a two-year research and development initiative to investigate the feasibility of Health*Connect* and to progress work on the national e-health building blocks (Health*Connect* 2002b, p. 2).

It has been a major Australian e-health initiative at a time when many similar developments were being considered by governments in Canada, the United States and Europe, in particular the United Kingdom. Such initiatives are accompanied by emerging, yet disputed, standardisation work carried out by bodies such as the International Standards Organisation (ISO), national standards bodies and a number of competing consortia of professional associations, technical and health specialists. The Australian health informatics community has been a prime mover in the international electronic health standards developments and in adopting the methodology of the Good European Health Record (GEHR) as the basis of the Good Electronic Healthcare Record and its successor, *open*EHR. GEHR was a significant research project which fed its findings into European standards.[1] One of the main features of the GEHR approach has been its focus on the exchange of health records or extracts thereof between health care facilities (such as clinics and hospitals) and across national boundaries. *Open*EHR refined the Good European Health Record object model by adopting its two-level modelling approach; the health record architecture itself and the clinical models or standards required for automatic processing of information. The latter has become known as the archetype system. Health*Connect* initially considered the *open*EHR as a possible implementation model (Health*Connect* 2003b p. 3). In the final Health*Connect* specification, the European CEN reference model that had major input from *open*EHR was adopted. As discussed later in this article, in terms of recordkeeping requirements, data models such as *open*EHR were difficult to map to records management or archival standards.[2]

Of key importance to initiatives such as Health*Connect* are the conceptual distinctions made between different types of health records in the electronic environment due to separate developments in research and standard setting, and differences in usage in the healthcare systems of different countries. In 2002 seven definitions were listed in the ISO electronic health records standards proposal document which stated that “a universally accepted definition of the ‘electronic health record’ does not exist” (ISO/TC 215 2002). The ISO definitions included the electronic health care record (EHCR), electronic patient record (EPR), computerised patient record (CPR) and electronic medical record (EMR). However, it was decided that for the purpose of the ISO, the term EHR would be synonymous with terms such as EHCR, CPR, EPR and EMR. In 2003 the international standards proposals defined the EHR simply as “a health record in computer processable form” (ISO/TC 215 2003). There was a recognition that diverse terms would continue in usage reflecting the needs of different health systems. In the United Kingdom, EPR and EMR were both focused on the patient’s treatment in one institution and captured in stand-alone medical records systems, while the EHR was beginning to be distinguished from other electronic records as the patient’s healthcare record from conception to death, distributed over a number of sites or aggregated at a particular source. In this sense the EHR

[1] The Good European Health Record project (1991–1995) was originally conceived as part of the European Community funded project (AIM project 2014), to address the major problem of interoperability of health information. The research team that proposed the Good European Health Record (GEHR) moved to University College London (UCL) in 1995 to establish the Centre for Health Informatics (CHIME). During the course of the GEHR Project, a project team was established under TC/251 of CEN, to propose a pre-standard health record architecture. This team, in which some members of GEHR participated, published the first CEN pre-standard, ENV 12265. GEHR delivered a significant advance in the application of object modelling approaches to the Electronic Health Care Record (EHCR). The GEHR approach was taken forward, beyond the United Kingdom and Europe, especially by Sam Heard, Tom Beale, Peter Schloeffel and their colleagues in Australia. In late 1999, a joint meeting of the Australian and UCL teams, in London, considered the forward pathway for the work of their two teams. The Australian GEHR methodology rested initially on the methods set out and followed for the first time in the GEHR project from 1989. It changed its name to *open*EHR (see Ingram 2002).

[2] The extensive EHR literature was examined at the commencement of the ARC project. The research did not find this literature relevant to a recordkeeping approach to EHRs.

was "longitudinal" and could be either a single encounter or a life time of healthcare (ISO/TC 215 2003). In the United States with its managed care system, EHR initiatives have been directed to EHRs with data exchange capabilities that can be shared electronically among doctors and other healthcare professionals caring for the patient, as well as insurance companies and hospitals (Terry 2004).

Health*Connect* adopted the following definition of the term EHR from The National Electronic Health Records Taskforce report:

> An electronic, longitudinal collection of personal health information, usually based on the individual, entered or accepted by health care providers, which can be distributed over a number of sites or aggregated at a particular source. The information is organised primarily to support continuing, efficient and quality healthcare. The record is under the control of the consumer and is stored and transmitted securely (Health*Connect* 2003a, p. 10; 2004a, p. 129).

In the final Health*Connect* specification, the EHR was defined much more simplistically as "a longitudinal collection of personal health information about a consumer, stored electronically" (Health*Connect* 2004a, p. 180).

The ISO electronic health records standards distinguished between the EHR that is shared as distinct from the providers' record by reference to a *local* and *shared* EHR (ISO/TC 215 2003). The local record of care may include externally sourced data, but is restricted to and owned by the health service provider (LEHR). The shared electronic record (SEHR) may be a summary record extracted from the "local" record or it may be summarised information incorporated into a primary carer's record.

Although Health*Connect* uses the term EHR, it positioned itself as a shared electronic health record (SEHR) project; in this project meaning a summary record extracted from a locally produced and maintained record of a health event. Event summaries would be stored in identified form and, subject to consent arrangements, made available to participating health service providers. The cumulating event summaries gathered over the course of numerous interactions with the health system would provide a longitudinal representation of an individual's health status. The event summaries would also be made available in either an identified or a de-identified form to authorised third parties including researchers and health administrators. These summaries were not designed to replace providers' clinical records.

Health*Connect* is also described as a system, but it is not simply a technical specification for software. To understand its complexity, it is essential to understand that it consisted of a suite of policies, strategies and records systems (Health*Connect* called these "building blocks"). The system was designed to operate at a cross-jurisdictional level that is working across the boundaries of all eight Australian States and Territories and the federal jurisdiction. Health*Connect* as a "system" includes governance, mandates, procedures as well as technical requirements and business specifications for a networked national health records system (Fig. 1).

The research analysis needed to address Health*Connect* as both a system and a project: governance and building of cross-jurisdictional records systems requiring co-operation at federal and state level; constitutional legality in terms of the control over health administration; privacy, ethical and legal aspects of participant consent in such a system; secondary research use of the data; appraisal, preservation and access; and business and technical system specifications for implementation. All of these issues are relevant to records and archival work.

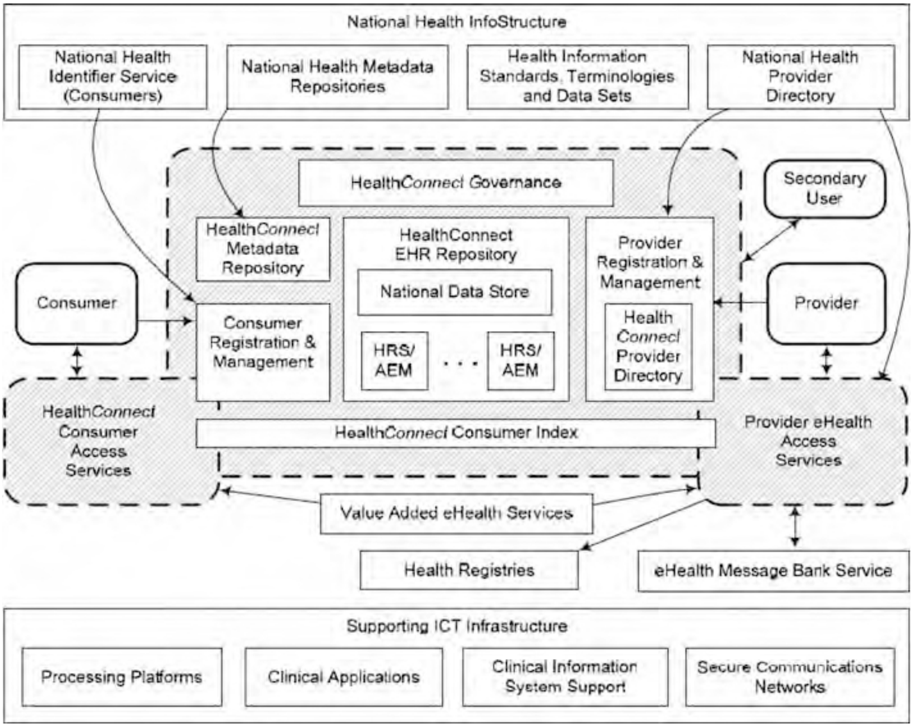
National Health InfoStructure
National Health Identifier Service (Consumers)
National Health Metadata Repositories
Health Information Standards, Terminologies and Data Sets
National Health Provider Directory
HealthConnect Governance
Secondary User
HealthConnect Metadata Repository
HealthConnect EHR Repository
National Data Store
Provider Registration & Management
Consumer
Consumer Registration & Management
HRS/ AEM
. . .
HRS/ AEM
Health Connect Provider Directory
Provider
HealthConnect Consumer Access Services
HealthConnect Consumer Index
Provider eHealth Access Services
Value Added eHealth Services
Health Registries
eHealth Message Bank Service
Supporting ICT Infrastructure
Processing Platforms
Clinical Applications
Clinical Information System Support
Secure Communications Networks

Fig. 1 Role Map for Delivery of Health*Connect* Services (Health*Connect* (2004a), p. 6). *Source*: Copyright of Commonwealth of Australia reproduced by permission

Health*Connect* has been a highly political and controversial initiative, in particular the privacy and consent aspects, and the millions of tax papers dollars spent on outsourced research investigations, legal consultancies, field trials and literally dozens of reports over 5 years, many of which have disappeared off its website. Health*Connect* extended beyond its original 2 year schedule, and still exists, although it now describes itself as:

> … a change management strategy funded through the Commonwealth Government and facilitated through a partnership with State and Territory Governments. Health*Connect* implementation aims to leverage existing eHealth projects and infrastructure, and progress towards compliance with National e-Health Transition Authority (NEHTA) and other nationally agreed standards to improve the availability of information in the health sector (Health*Connect* 2008).

Many of the Health*Connect* initiatives have continued within the National E-Health Transition Authority Limited (NEHTA), a not-for-profit company established by the Australian, State and Territory governments to develop better ways of electronically collecting and securely exchanging health information. NEHTA is funded until mid-2009 to continue the work commenced in Health*Connect* on business requirements, interoperability frameworks, and particularly to progress three key initiatives identified as critical infrastructure in the earlier project: a national clinical terminology, a national individual identifier for healthcare purposes and a national healthcare provider identifier (National E-Health Transition Authority 2007, p. 4).

Research scope and framework

Health*Connect* represented a very complex, politically sensitive system with an array of governance, regulatory, ethical and recordkeeping issues that required attention. While Health*Connect* itself had identified a number of building blocks that must be put in place to underpin the system, including development of the legal data protection and security frameworks necessary to facilitate electronic transfers of health information (National Electronic Health Records Taskforce 2000, p. 19), a systematic analysis of the legal, ethical and recordkeeping perspective was missing. With its extensive research and development phases over several years, Health*Connect* provided an opportunity for the research team to examine issues relevant to responsible recordkeeping, disparate jurisdictional legal regimes and the ethical impact on long established health professions. In particular, the project focused on how to preserve trust and confidentiality in patient–doctor communications in interactive systems; ensure the privacy of patients and health practitioners while retaining the integrity of health records and provide significant legal, ethical and recordkeeping strategies for reliable and authentic networked health records over time.

The research design consciously adopted a framework for analysis based on the records continuum model. That is, health records should be managed for as long as they are of value to organisations or to society, addressing their creation, capture, organisation and access over time, and their role in constituting personal, corporate and collective memory. There was a concerted effort by the ARC team to engage with the Health Information Management Association of Australia in relation to the application of the records continuum model to the project. This included explaining to health records managers and health informatics specialists why archivists are interested in health records in and through time and space, and how the model could assist them in developing broader records strategies.[3] In the context of this project the model provided a test case for assessing the usefulness of the theoretical models in practice.

Health*Connect* provided a multi-jurisdictional, cross-organisational exemplar for complex transactional systems operating in distributed networked environments increasingly using service-oriented approaches. The records continuum model's capacity to embrace multiple simultaneous views of records enabled analysis of the individual components of the highly complex system proposed. For example, the records continuum's fourth dimension operates in a region that overarches individual organisations. Many of the core Health*Connect* records were operating in a pluralised space from the time of their creation, thus enabling application of the recordkeeping concerns of the fourth dimension to be applied to Health*Connect* records regardless of the dimension in which analysis

[3] While in Australia health records management professional work and education are separate from records management or archival practice, there has been collaboration in the past between the Public Record Office of Victoria and the Health Information Management Association of Australia (HIMAA), for example, in 1987 they jointly developed a disposal schedule for public hospital patient case files for Victoria (see Kearsey 1989). In relation to the ARC project, one of the research associates was a health records manager who acted as a bridge between the research team members and the health records professions. Two presentations on the research framework by the project's Chief Investigators took place at the 2003 HIMAA national conference, and a refereed publication was accepted in 2004 in the HIMAA journal. The article presented at the conference on the records continuum model was well received (Iacovino 2003). The Health Informatics Society of Australia also attended the 2003 presentation. The records continuum model was also presented to law and health professionals at 28th International Conference on Law and Mental Health, International Academy of Law and Mental Health, Sydney, 1 October, 2003. A national symposium on the interim research findings organised by the research team in Melbourne was advertised and attended by HIMAA members in 2004.

might otherwise "place" them. Similarly, the model facilitated analysis of complex sets of multiple creating agents in different locations at different times. The model provided a testable framework for developing clear and consistent analysis of recordkeeping concerns across the complex layered technical architecture developed for Health*Connect*, demonstrating its utility as an analysis tool in such emerging information structures.

Within a records continuum framework, it was possible to distinguish between a patient's SEHR created from point of care source systems for use by authorised persons and an EHR created, received, maintained and owned by a health service provider at the point of care, which may also incorporate records derived from SEHRs (Fig. 2). To ensure that the most reliable and authentic patient record would be preserved, the relationship between the shared record and its sources was a critical issue.

A recordkeeping reading of the technical architecture of Health*Connect* by the research team identified the Health*Connect* SEHR as a cross-organisational shared record within a distributed model of regional repositories responsible for recordkeeping actions across organisations. The source record, from which individual event summaries were to be extracted, would remain the individual record in the originating clinical records system. The SEHR itself was a separate record, stored in one of a network of federated distributed repositories known as Health Record Systems (HRS) and replicated in a centralised National Data Store (NDS). The aggregated view of the individual summary records presented to the health care provider at the point of care was again another record which was of the most critical concern, because it provided the information within the Health*Connect* system for the health care provider's decision-making (Reed 2004). All these records needed to be reliable and authentic for their own purposes. Therefore, the research needed to address which data stores contained records to be regarded as primary, original, complete and authentic (Iacovino 2004a).

The issues of privacy, confidentiality and ethics raised by electronic networks and the adequacy of the existing legal and regulatory framework were also examined within the

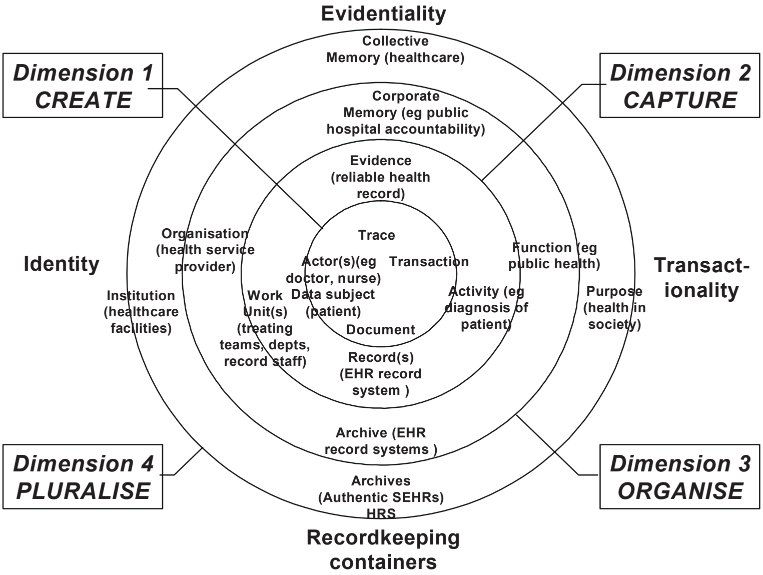
Evidentiality
Collective Memory (healthcare)
Corporate Memory (eg public hospital accountability)
Evidence (reliable health record)
Trace
Dimension 1 CREATE
Dimension 2 CAPTURE
Identity
Organisation (health service provider)
Institution (healthcare facilities)
Actor(s)(eg doctor, nurse)
Transaction
Work Unit(s) (treating teams, depts, record staff)
Data subject (patient)
Document
Function (eg public health)
Activity (eg diagnosis of patient)
Purpose (health in society)
Transact-ionality
Record(s) (EHR record system)
Archive (EHR record systems)
Archives (Authentic SEHRs) HRS
Dimension 4 PLURALISE
Dimension 3 ORGANISE
Recordkeeping containers

Fig. 2 Records continuum model: SEHR and EHR. Copyright FrankUpward and Livia Iacovino 2004

records continuum model in which these concepts are analysable within one time-space module. For example, the issue of privacy includes not only how private information is captured, used and disclosed but also when it is destroyed or preserved and made accessible both during the life and after the death of the patient.

Research design and methods

The recordkeeping research in the project took account of significant research in the archives and records community on the preservation of authentic and reliable electronic records over time. For example, *Recordkeeping Metadata Standards for Managing and Accessing Information Resources in Networked Environments Over Time for Government, Social and Cultural Purposes* had focused on developing metadata standards for records within evolving international or national generic metadata sets (Monash University 1999). Its major outcome has been a high-level recordkeeping metadata schema (RKMS). The *International Research on Permanent Authentic Records in Electronic Systems (InterPARES 1) Project* was an international research initiative focused on the long-term preservation of inactive authentic electronic records. Its outcomes included an authenticity template for the systematic analysis of electronic records and systems and technological methods for preserving authenticity (InterPARES 1 Project 2001). Another Australian project was the *Victorian Electronic Records Strategy* (VERS) which is concerned with the long-term preservation of electronic records in a long-term record format (Public Record Office Victoria 1998). A significant outcome of all these projects had been the recognition of specific differences in the application of authenticity standards and the need to test these in discrete environments such as the health context.

Due to the complexity and evolving nature of the Health*Connect* project, the ARC research objectives had to be focused not only on the various iterations of the system design but also on governance which remained significantly unresolved during the research. Health*Connect*'s lack of a finalised governance structure impacted on all aspects of the project but was particularly significant in relation to ownership issues and records retention. The sharing of electronic health information amongst healthcare professionals and their patients and third parties highlighted the need for the preservation of the shared health record for at least the life of the patient, and possibly beyond. Health*Connect* had clarified that the ownership of doctors' medical records would not be affected by the proposed system, but it did not address the issue of the ownership of the HRS held within the federated model, provider information in the shared summaries and the regulatory regime that would apply to the shared records.

Therefore, the project had to address significant legal, ethical and recordkeeping gaps in Health*Connect*'s policies and business architecture. In order to identify these gaps, it analysed the recordkeeping functionality of three versions of the business and technical architecture over the period 2002–2005, and as part of this process identified critical issues of social and legal concern (privacy, confidentiality, consent, duty of care and ownership of information) that needed to be addressed either as part of the business and technical specifications or through policy or law reform. The research examined the ownership of records in different parts of the system (Iacovino 2004a, p. 53) and whether doctors who participated in the proposed scheme could ensure their duty of care to their patients (Mendelson 2004).

In relation to health confidentiality the research began with the premise that legal confidentiality in Australia had already been strained in relation to health records. This starting point arose from the large number of Australian Federal and State laws that mandate disclosure of medical information (Mendelson 2003; Paterson 2004; Iacovino 2006). In the case of privacy, it examined the impact on health privacy of health identifiers; records retained for the life and beyond of the patient and participant consent, in particular, the extent to which the system remained voluntary for both the patient and the practitioner, as consent to collect, use and disclose personal information is a basic privacy principle (Paterson and Iacovino 2004). A mental health case study examined the ethical, legal and recordkeeping issues of enabling third party access to shared electronic mental health records, in particular the capacity of a mental health patient to consent to participate in the system, and ethical theories that could equally be used to support respect for privacy as for respect for confidentiality (McSherry 2004a, b). Although the research team found that mental health services could benefit from the sharing of information between health care providers, there was a paucity of specific measures in the Health*Connect* proposals and in the evolving EHR standards to differentiate mental health from other health information (Iacovino 2004b).

Recordkeeping research focused on the mapping of recordkeeping principles and standards to the business architecture concentrating on issues of reliability and authenticity while supporting confidentiality and privacy. Who ultimately would control the SEHR remained of fundamental importance to its preservation and its authenticity. It appeared that by default it would be the Australian federal government, but issues of ownership of different parts of the system remained unresolved. In addition cross-jurisdictional issues were addressed, for example, whether the Australian Draft National Health Privacy Code would apply to all states (Paterson and Iacovino 2004). Thus, the recordkeeping research design took account of the legal and ethical analyses undertaken contemporaneously with the recordkeeping aspects of the project.

Recordkeeping research tools

The recordkeeping research needed to adopt benchmarks that would provide valid findings in terms of records and archival issues, as well as legal and ethical ones. To begin with recordkeeping research methods and tools for identifying the most reliable and authentic records in complex cross-jurisdictional systems are underdeveloped. Benchmarks for reliable and authentic records adopted by the project included RKMS, the authenticity requirements and the preservation model of the InterPARES 1 and the standards for archiving electronic records in VERS. On the general level there was also the *International Standard ISO 15489-1, Information and Documentation, Records Management,* Part 1: General; *ISO 15489-2, Information and Documentation, Records Management,* Part 2: Guidelines and *ISO 23081-1, Records Management Processes: Metadata for Records*, Part 1: Principles.

Two major research tools were developed for the recordkeeping analysis. These then generated a number of analysis products, reported below, and provided input into the analysis of privacy, ethics and consent undertaken in different parts of the project. The first research tool was intended to be a mapping of the Health*Connect* business architecture metadata requirements to emerging recordkeeping metadata sets to enable assessment of adequacy. However, the initial presumption of granularity in the business architecture of the system was later found to be insufficient to map to metadata sets such as RKMS. Instead a generic shared health records implementation standard (*open*EHR) was mapped to a records standard (VERS).

The second research tool was a recordkeeping analysis of the technical specifications and business architecture of Health*Connect*. This was done three times across the course of the project to reflect the evolution of the published specifications.

VERS system requirements and *open*EHR

*Open*EHR is an open standard for the design of EHRs consisting of a number of data models. It had provided major input into international EHR standards, and it had been tested in lead sites for a small-scale version of a full-shared network for Health*Connect*'s requirements (Health*Connect* 2003b, pp. 37–38). For these reasons it was selected by the ARC research team for mapping elements that it directly supported in VERS to test its recordkeeping compliance (Meredith 2004). VERS is an electronic records standard adopted by the Victorian State Government for electronic records submitted to the Public Record Office Victoria in the form of VERS encapsulated objects (VEOs). The analysis covered the elements in *open*EHR that either directly supported or could be made to support the derived VERS requirements (Table 1).

The research concluded that *open*EHR is an implementation standard that has the potential to be VEO compliant if additional metadata elements were added. It had limited overall compliance with recordkeeping requirements. Generally, the *open*EHR model fell short of recordkeeping compliance in areas addressing recordkeeping processes such as managing disposal and retention and in documenting recordkeeping mandates. The concept of the *open*EHR audit trail needed to be extended to include record access as use in addition to creation, modification and deletion. *Open*EHR also sidestepped the important issue of the long-term preservation of records by leaving the most important aspects of the mechanism for ensuring this up to system developers.

Table 1 VERS system requirements and *open*EHR compliance

Requirements derived from VERS system requirements specification	*open*EHR compliance
Record authenticity	Depends on access control models, yet to be documented
Record integrity	Partial
Document conversion	Not applicable
Metadata capture	Partial
Modifying information associated with records and folders	Full
Documenting the history of the records and folders	Partial (record creation and modification, but not access)
Reliability	Depends on implementation
Refresh	Depends on implementation
Records transfer	Not applicable

Mapping recordkeeping standards to technical specifications and business architecture

The major recordkeeping research tool adopted in the research project was the analysis of the Health*Connect* technical specifications and business architecture. This analysis initially merged multiple documents to compile a description of processes which was as complete as possible. From the process descriptions, recordkeeping requirements were derived, identifying information entities, assessing where in the architecture proposed the record would reside, identifying any key recordkeeping standards (using the project benchmarks listed above) that were relevant to the requirements and identifying recordkeeping, legal, privacy and ethical issues that were raised.[4] The changes to the technical specifications and business architecture which occurred over the period of the research project were inevitable in such a complex project, but a frustration to the research team who spent considerable time re-doing analyses against newer specifications. There was a constant need to update and revisit work through three versions of the Health*Connect* business and technical architecture models that often introduced subtle but significant changes. All three versions of the business architecture could thus be compared and served as the raw data for qualitative and quantitative analyses to support a number of research products for the project team (Table 2).

The recordkeeping analysis provided many detailed findings focused at individual process levels which were consolidated into an issues report (Reed 2005a) and a governance matrix (Iacovino 2005). The discussion below reflects areas of the Health*Connect* conceptual design that are of potential relevance to other complex cross-jurisdiction transactional systems.

It was clear from the specification that the SEHR was a logical rather than a physical record, and the specification clearly identified at least nine different components which contribute to a single SEHR (Health*Connect* 2004a, pp. 129–130). Each of the components may or may not be physically held in the same database and each had different means of compilation, whether that be through manual contribution, automatic extraction and ingest or by system logging (for example, in the case of version logs, access logs or audit trails).

Recordkeeping issues arising from the complex federated networked system architecture

As described in Fig. 1, the Health*Connect* system incorporated a national layer (NDS) which provided consolidated storage of all event summaries ingested and maintained in local nodes. These local nodes potentially reflect individual states or regional jurisdictions and are called Health Record Systems. The HRS act as the storage and collection point of individual event summaries obtained through interfaces and transfer protocols sitting on top of the individual clinical or health care systems which are maintained by health care providers. In this complex architecture design, data (and potentially the same data) is stored in each of the layers. The data is likely to be under different jurisdictional requirements: the NDS at Commonwealth level, the HRS at state or regional levels and the

[4] The initial analysis using the Business Case System process specification version 0.7, March 2002 (Health*Connect* 2002a) was updated to reflect the Business Architecture v1.0 released as Volume 3.6 of the Health*Connect* Interim Research Reports, April 2003 (Health*Connect* 2003d). The final mapping analysis was completed by Barbara Reed using Health*Connect* Business Architecture Version 1.9, November 2004 (Health*Connect* 2004a) and the Specification of Health*Connect* Business Requirements, 2004 (Health*Connect* 2004b). Peer review was undertaken by Livia Iacovino as a Chief Investigator and Hans Hofman, who has specialised knowledge of data modeling and electronic recordkeeping.

Table 2 Example of a single process specification extracted from Consolidated Analysis Spreadsheet 2005

Analysis category	Analysis
Health*Connect* Business Architecture 1.9	B: Manage Health*Connect* participation
Processes	Process B3: contracting with health providers for use of Health*Connect*. Individual providers and provider organisations ("providers") must enter into agreements with the Health*Connect* governing body in order to use Health*Connect*
Expression of requirements	C-73: in progressing process B3 (contracting with providers for use of Health*Connect*), the Health*Connect* governing body should (a) with legal advice, develop standard agreements for providers, that incorporate observance of Health*Connect* rules as promulgated by the Health*Connect* governing body from time to time; (b) negotiate the final form of the provider agreements and initial Health*Connect* rules with stakeholder bodies; (c) establish processes for provider registration that involve provider organisations and individual providers entering into their respective agreements and being instructed on their obligations; (d) set up processes to monitor compliance with provider agreements; and (e) on occasions, enforce conditions in these agreements.
Derived recordkeeping requirements	Standard agreements Individual licences/legal agreements Monitoring compliance records Enforce compliance records
Information entities	Applications for secondary use, decisions made on them, information about implemented processes for this
Information store	Health*Connect* level (i.e. associated with the administration of Health*Connect* itself, not its federated hubs, the technical health records systems or any of the contributing systems)
Standards relevant	ISO 15489.1: 9.1 Determining documents to be captured into a record system: business or personal actions should be captured as records and linked with metadata which characterise their specific business context when they commit an organisation or individual to action, render an organisation or individual accountable, or document an action, a decision, or decision-making process
Legal/ethical issues	Health*Connect* participants will be obliged to abide by privacy legislation and by specific Health*Connect* privacy rules. The National Health Privacy Code will be used when it has been implemented, until then privacy arrangements will be tailored to suit each jurisdiction for each implementation, with a view to working towards a single national set of rules (BA v1.9, p. 78)
General issues	Participating organisational systems and personal provider IT devices must be demonstrably compliant with appropriate published security policies and standards that have been endorsed by Health*Connect* (BA v1.9, p. 35) Software developed to interact with Health*Connect* records systems will be tested and accredited to the standard endorsed by Health*Connect* (BA v1.9 p. 35) Responsibilities of Health*Connect* providers include commitment to providing accurate information to Health*Connect*, recognition of consumer rights as participants in Health*Connect*, participation in line with Health*Connect* confidentiality and privacy agreements, local procedures which comply with appropriate national standards to meet Health*Connect* privacy and security requirements. These will include processes to control access to, and audit the use of, the organisations' information system; using clinical information systems to access Health*Connect* that comply with the technical requirements of Health*Connect*; maintaining security of any EHR information integrated into their clinical information systems (BA v1.9, p. 77)

individual clinical or health care systems with public hospitals or private health care providers. Issues of synchronisation across the systems and clear identification of where the authoritative record resides were critical recordkeeping concerns.

Which data stores contain records to be regarded as the primary, original, complete and authentic record? The Health Record System layer was determined to be the authoritative source for all of an individual's EHR; however, there is a requirement on the HRS to transmit copies of all event summaries to the NDS, within 24 h of an EHR being updated (Health*Connect* 2004a, p. 110). 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" (Health*Connect* 2004a, p. 131). This could be understood 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 NDS for long-term storage and retention (Health*Connect* 2004a, p. 155).

The individual clinical or health care systems of public hospitals or private health care providers should have had the implicit "best", most reliable records reflecting the instance of the health care event. Synchronisation of data between the HRS and various applications was not guaranteed, creating some uncertainty about the reliability and completeness of the record maintained in the HRS. The system would need to synchronise the summaries entering the HRS with applications maintaining patient details and with the local practice record to ensure data accuracy.

On the other hand, an argument could be made that the authoritative record was to be regarded as the record in the NDS, a logical assumption as this is the version maintained for archiving and long-term storage purposes. This led to the conclusion that synchronisation of multiple data stores containing variations or versions of the same information will need careful management. In order to maintain assertions of authenticity, reliability and integrity, records of the transmission processes will be needed to ensure that verification can be proven.

The process of identification of the information entities (or data) that would be created, used, amended in the different processes, and where the information resided and who was responsible, was not always clear. Would the roles and responsibilities associated with the different layers and different copies of the same data be clearly identified and delineated? The research team sought to identify the information entities used in the system and to locate where they were created and stored, how they were managed and who was responsible. An analysis of the dataflow(s) in the Health*Connect* system found that there was clearly a risk that information may be lost, not carefully managed, or exist in more than one place without knowing what the authoritative source or version was (Hofman 2005). Apart from the identification of information and its flow and residence, the analysis identified synchronisation issues as much information would be resting at the same time in different places, completely or partially.

In addition to requirements to disentangle ownership and responsibility issues for records at various layers of this complex system architecture, a further complication for recordkeeping was added with each layer of the architecture performing specific functions on the SEHR, requiring further recordkeeping. Thus, the NDS provided functionality associated with mediating and delivering access to secondary users, either in de-identified form or in specific instances as identifiable data. The HRS was the source for clinical providers to obtain aggregated views which were consolidated (or not) into their local clinical systems in order to provide point of service care. Corrections to the event summaries could be made by clinicians. Individual patients would be encouraged to contribute to their evolving record of health. Each of these instances was a recordkeeping event associated with the HRS beyond the initial ingest of an event summary. Recordkeeping events associated with these specific areas of functionality were not well defined in the specifications.

Archiving and retention

As governance of the Health*Connect* had not been determined, it was uncertain which regulatory regimes would apply. If the summary records within the NDS were deemed to be Commonwealth records, then the responsibility for them would be with the National Archives of Australia operating under federal law, regardless of the fact that they were replicated from the HRS operating in state or territory jurisdictions with quite distinct recordkeeping, privacy and potentially consent requirements. This whole issue was never clearly identified or clarified in the documentation leaving large issues of regulatory responsibility and compliance unresolved. Only version 2002 of the functional and technical requirements included rules for archiving event summaries according to type, age and compliance with archival legislation (Health*Connect* 2002a, p. 131). The 2003 system architecture included "archiving" as "the capability to archive EHR and audit data" (Health*Connect* 2003a, p. 34). The Health*Connect* business architecture broadly referenced the need for rules for archiving event summaries but did not adequately address records retention, in particular the disposal of specific recordkeeping process actions for records created at different layers in the system.

The NDS is clearly identified as the component of the Health*Connect* architecture that would have been responsible for the long-term retention of the SEHR (Health*Connect* 2004a, p. 7). This key design principle then allows individual Health Record System implementations to destroy records with confidence once they deem it appropriate (not withstanding 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.

Indeed, the research team concluded that the specification of functionality for the NDS was significantly underdeveloped, with emphasis on defining functionality for the HRS and the interaction of data between layers.

Audit trails as recordkeeping

The inclusion of audit trails to monitor access was a key component of the system. Audit trails were also the primary mechanism available in the Health*Connect* specification to meet recordkeeping requirements. It is clear in the specification that the audit trails/logs are to be linked persistently to an individual SEHR by means of the unique identifier, thus providing a much more contextually grounded record. However, the audit log would potentially be physically created and stored at a number of layers within the Health*Connect* technical architecture, including the registration layer (Health*Connect* 2004a, p. 146) and the HRS (Health*Connect* 2004a, p. 112).

Each layer is instructed to dispatch the access logs to the NDS, which then manages a "consolidated" access log (Health*Connect* 2004a, p. 157). There is a lack of clarity about whether the NDS's own audit and access logs are incorporated into this consolidated access log and how consumer access is gained to this record. While the emphasis on being able to query transactions relating to access reflected the overwhelming public concern on access, equally all transactions relating to the cumulative record would need to be logged in a similar manner and persistently linked to the record in order to meet recordkeeping concerns. Some of this notion was incorporated in 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" (Health*Connect* 2004a, p. 156).

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 the Health*Connect* 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. It is more common for audit logs to be used as system tools to provide backup or recovery when required. However, all instances of all transactions (including system administration, reporting and secondary uses) conducted on any part of the SEHR 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 missing in the consideration of the audit trail/access log as a recordkeeping tool in Health*Connect*. Overall, this technique only addresses the data components of the SEHR, while records occur throughout the other supporting business processes specified in the business architecture. Different means of achieving an appropriate recordkeeping outcome might have been achieved if a recordkeeping perspective had been available as a partner to the design. Certainly, retaining all audit trail data relating to an individual SEHR indefinitely was one which should be subject to considerable future scrutiny.

Metadata schemas

Event summaries are a specified set of data extracted from individual clinical systems in a standardised metadata template. Views and lists which control what a clinician can see from the SEHR at the point of service delivery are also governed by metadata templates. The system architecture specified the requirement to maintain generations of metadata templates for event summary content formats or metadata schema associated with event summaries. It recommended XML technologies be used to develop extensible metadata schema for this purpose, but it did not address what needed to be extensible in addition to the data content and format if the record was to be understandable over time. The analysis found that the SEHR would only be meaningful if the business rules, common services (standards and legislation), as well as the directory identification information, and data dictionaries from the national level had been persistently linked with the relevant summary; for example, the record must have a persistent link to the consent rule operating at that time the record was created. A central access control authority manages access to records established under different rules (Health*Connect* 2003d, p. 78). Provider and organisation directories are supporting services that reside outside of the HRS proper (Health*Connect* 2003a, pp. 31–32). Thus, relevant metadata conceptualised for implementation in the national coordination level also needed to be preserved with the HRS record, located at another "node" within the federated system.

The 2004 business and technical architecture sought to reconcile "the many different positions on Health*Connect* held by Australian, state and territory health jurisdictions, consumer and privacy advocates, health service delivery organisations, healthcare providers and the health software industry" (Health*Connect* 2004a, p. 14).[5] The requirements for standard forms, expressed in the form of XML metadata templates or incorporated into schema definitions or stylesheets, had been identified as critical infrastructure in all electronic health processes by Health*Connect*. The continually evolving picture of standards included the HL7 messaging protocols, the CEN EN13606 reference model, the research initiatives of *open*EHR and archetypes, all of which recognised the importance of a standardised definition and expression of data elements constituting the health record (Health*Connect* 2004b, p. 71). The business architecture identified that each SEHR event summary, view, list, query should be tagged with the metadata version of the template that created it and that each version of the templates would need to be maintained in the long term, to enable continuing accessibility and meaning to be attributed to records submitted according to superseded templates (Health*Connect* 2004a, pp. 144–145, 156). Similarly, the requirement to maintain cumulative records of changes to encoding schemes, for example, SNOMED, used to derive data values are all recordkeeping issues for record integrity (Health*Connect* 2004a, p. 126).

Access mechanisms

The analysis found that the sophisticated consent control mechanisms included in earlier versions of the business architecture and research reports (Rooney and Aitken 2002; Health*Connect* 2003c) were simplified with each version of the business architecture. The initial articulation of the consent control mechanisms had 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 (for example, 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. The 2004 version of the business architecture referred to a secure area for sensitive information, such as a "secure envelope" which stores health information the patient may not want revealed, but this was relegated to the "future" on the basis that it required further research (Health*Connect* 2004a, pp. 3–4, 55, 172). Technical constraints and ease of technical implementation seem to have influenced the management of consent and access in the evolving business architecture. A much simpler one-dimensional model was proposed in the final version deferring the complexity until subsequent post implementation development (Health*Connect* 2004a, p. 32).

Health*Connect* used the concept of EHR lists or views to assist health service providers interrogate the health data. EHR lists or views are tailored sets of data compiled across many event summaries relating to a single person or compiled across many event summaries relating to many individuals. These are generated automatically and stored within the Health Record System. The analysis found that these are records in their own right and will need to be managed as such—they will need versions and dates. A preliminary indication that this issue was appreciated was included in the specifications (Health*Connect* 2004a, p. 137). 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

[5] Health*Connect*, Business Architecture v1.9, Nov. 2004 remained publicly available until early 2006 but has since been withdrawn from the Health*Connect* website. It was intended to be the consultation draft for the first full implementation of Health*Connect*.

transmission details of whom they were sent to and when. Their representation as views or lists is not discussed in the specifications as a process separate to that of access, with the exception of secondary use.

Registration of health care providers in the system

Registration as a process is a key recordkeeping function. The project analysis found that the proposed outsourcing to the private sector of the management of registration functions (Health*Connect* 2004a, p. 156) was not only a privacy concern but from the recordkeeping point of view sat outside the EHR records system per se. For example, an organisation running the Health*Connect* Consumer Access Services (HCCAS) gains access to the Consumer Index and message handling and transport applications. In addition the private delivery of the individual HRS would be run by "Approved EHR Managers" (AEMs) (Health*Connect* 2004a, pp. 110–111, 115–117, 163). Embedded in the private delivery of services were significant recordkeeping requirements: agreements such as those envisaged with AEMs or HRS functionality, contractors, or those providing services. The list of proposed responsibilities for security and access control by AEMs included a significant recordkeeping responsibility (Health*Connect* 2004a, p. 112). For the SEHR to be meaningful over time and to maintain its required characteristics of authenticity and reliability, the persistent linkage over time to identification of health care providers is essential. The interaction of crucial data between private providers and the Health*Connect* layers, management responsibilities and protection across time is unspecified.

Statistical analysis

The research project's spreadsheet that captured the processes in the business and technical architecture was also used to analyse the statistical occurrences of key records standards found in the Health*Connect* processes to ascertain the extent to which the 2004 business and technical architecture reflected recordkeeping best practice (Reed 2005b). The key industry standards were

- InterPARES 1 Project, "Requirements for Assessing and Maintaining the Authenticity of Electronic Records", 2001.
- ISO 15489, International Standard on records management, Parts 1 and 2, 2002.
- ISO 23081, Records management processes: metadata for records, Part 1: principles, 2005.

These industry standards were considered the most authoritative statements of recordkeeping available at the time of the research. They were seen as complementary; the international standard focusing on principles and processes required for good recordkeeping, while the InterPARES benchmarks and baseline requirements provided particular statements of characteristics to be sought in relation to assertions of authenticity of electronic records.

Each process description and derived recordkeeping requirement from the Health*Connect* business architecture was analysed to assess which, if any, recordkeeping standard requirement was relevant to the process. For many of the business processes being described, multiple sections of the recordkeeping standards were identified as being applicable. For some processes, it was not possible to find an appropriate recordkeeping standard.

InterPARES 1 requirements for assessing and maintaining the authenticity of electronic records

The InterPARES project devised two sets of criteria:

- The benchmark requirements supporting the presumption of authenticity of electronic records devised to test the presumption of authenticity of records belonging to the creator of the records in their current electronic systems.
- The baseline requirements for the production of authentic copies of electronic records devised to support assertions of authenticity once the records have been removed from the creating environment, thus creating "copies" of the original records.

Of the possible eight InterPARES benchmark requirements, mappings were made through the analysis to all eight of the requirements as detailed in Table 3, indicating that issues were addressed.

As indicated below, the benchmarks are used to weigh statements of authenticity in the creating environment. The percentage figures indicate the relative presence of these requirements against the process definitions and specifications mapped. These percentages are to be treated with some caution, as not every process definition or specification will be relevant to the specific InterPARES benchmark issue. They do, however, provide sufficient basis for an indicative assessment.

Using the stated criteria for use of the InterPARES benchmarks, it was possible to make some general assessment of the degree to which authenticity can be asserted. That is "a presumption of authenticity will be based upon the number of requirements that have been met and the degree to which each has been met. The requirements are, therefore, cumulative: the higher the number of satisfied requirements and the greater the degree to which an individual requirement has been satisfied, the stronger the presumption of authenticity" (InterPARES 1 Project 2001, Appendix: requirements for assessing and maintaining the authenticity of electronic records, Sect. 1.2.1: The presumption of authenticity). The following assertions were made from the InterPARES benchmarks:

- That issues of documentary form, access and authentication are potentially adequately addressed in the Health*Connect* specifications.
- That the remainder of the requirements falls short of sufficiency to be able to assert authenticity.

Table 3 Instances of mappings made to InterPARES benchmark requirements

InterPARES benchmark requirement no.	Summary of requirement issue	Instances of mapping	Percentage against available 96 processes and specifications (%)
A5	Documentary form	35	36
A2	Access	31	32
A6	Authentication	23	23
A8	Documentation at removal or transfer	8	8
A4	Protective procedures—integrity over changes media and technology	8	8
A3	Protective procedures—corruption of records	8	8
A1	Integrity	4	4
A7	Authoritative record—multiple copies	1	1

- The ability of each of the InterPARES benchmark requirement to be mapped at least to some requirements in the Health*Connect* specification indicates that the Health*Connect* system should be able to accommodate the requirements.
- That the developers of the Health*Connect* specifications should use the InterPARES benchmark requirements to further incorporate the requirements to enable a much more robust assertion of authenticity.

The baseline requirements outline minimum conditions necessary to enable the preserver to attest to the authenticity of inactive electronic records. The baseline requirements build in a set of presumptions about recordkeeping that are not necessarily suited for application in a cross-organisational networked electronic system. Rather the presumption is that electronic records are being removed from the creator into a preservation system. None the less, while the language and angle of the baseline requirements is somewhat different, the requirements that are specified should be valid for a system like Health*Connect* where records are being transmitted and stored in locations away from the originating system (that is in designated HRSs or in the NDS under the aegis of the Health*Connect* governing body, either or both being different to the creator's system, and that of the individual practitioner or health care provider).

The baseline requirements address three areas:

B1—controls over records transfer, maintenance and reproduction
B2—documentation of reproduction process and its effects
B3—archival description

It was anticipated that a match would be found between B1 and B2 and the Health*Connect* specifications. Notwithstanding the statement in the InterPARES Authenticity report that "all the requirements in the baseline requirements must be met before the preserver can attest to the authenticity of electronic records in its custody", for Health*Connect* and the purposes to which the analysis was adopted, the research team asserted that a robust degree of correspondence between requirements B1 and B2 would meet authenticity requirements. Of the three requirements, B1 has three subsections and B2 four subsections. The findings detailed in Table 4 were that mappings could only be found against B1, although a number of the Health*Connect* requirements could be more specifically mapped to B1b (security and control procedures are implemented and monitored).

Thus, we can assert that the Health*Connect* specification would not meet the InterPARES baseline requirements for authenticity. Although given that the baseline requirements have been taken into a different context it is not unrealistic to assert that the findings above indicate that the Health*Connect* system architecture could probably meet the requirements. It was possible to conclude that the developers of the Health*Connect* specifications should use the InterPARES benchmark requirements to further incorporate the requirements to enable a much more robust assertion of authenticity.

Table 4 Instances of mappings made to InterPARES baseline requirements

InterPARES benchmark requirement no.	Summary of requirement issue	Instances of mapping	Percentage against available 96 processes and specifications (%)
B1	Records transfer	19	
B1b	Records transmission	16	
		35	36

ISO 15489.1, Records Management Standard

ISO 15489 consists of 10 major clauses. Within each of the 10 clauses further subclauses are identified. The mapping has been done to the subclause level (Table 5).

In relation to ISO 15489.1 Records Management Standard, clauses 1–5 of the ISO 1489 are introductory clauses covering scope, references, terms and definitions, benefits of records management and regulatory environment. Therefore, it was not surprising to find no direct mappings against these clauses. The statistical analysis did not find appropriate mappings for records characteristics such as authenticity and useability (ISO 15489, 7.2.2 and 7.2.5), with minimal mappings for authenticity and reliability (ISO 15489, 7.2.3 and 7.2.4). Similarly, the absence of any mappings to records system characteristics of reliability and integrity are of concern (ISO 15489, 8.2.2 and 8.2.3). These critical recordkeeping characteristics would have determined trust and robustness of the system. Very minimal mappings were able to be made for every one of the recordkeeping processes outlined in clause 9 of the ISO 15489 standard. This finding provided support to the assertion that Health*Connect*, despite being an electronic records system, does not incorporate recordkeeping requirements into the business requirements to an adequate degree.

Table 5 Instances of mappings made to ISO 15489.1 Records Management Standard

ISO 15489.1 clause no.	Summary of content of section	Instances of mapping	Percentage against available 96 processes and specifications (%)
6.1	Policy and responsibilities—general	1	1
6.2	Policy and responsibilities—policy	1	1
6.3	Policy and responsibilities—responsibilities	1	1
7.1	Principles of records management programs	1	1
7.2.3	Reliability	1	1
7.2.4	Integrity	1	1
8.1	Design and implementation of a records system—general	1	1
8.3.2	Documenting records transactions	37	38
8.3.3	Physical storage medium and protection	1	1
8.3.4	Distributed management	15	16
8.3.6	Access, retrieval and use	1	1
8.4	Design and implementation methodology requirements for records capture	3	3
9.1	Determining which documents to be captured into a records system	8	8
9.2	Determining how long to retain records	3	3
9.4	Registration	8	8
9.5	Classification	2	2
9.6	Storage and handling	6	6
9.7	Access	18	19
9.8	Tracking	3	3
9.9	Implementing disposition	1	1
10	Compliance monitoring	6	6

This could be the case for other large-scale EHR systems and could be used as a model to test other similar systems.

ISO 15489.2, Records management, Part 2: technical specification

Health*Connect* requirements were mapped to ISO 15489.2 where a more adequate or precise representation of the issue could be identified in that part of the standard (Table 6). The analysis therefore complements the analysis of ISO 15489.1 detailed above.

In the mappings to specific issues within the technical specification, two issues were clearly the most prominent:

- Access (consolidated 65 instances)
- Backup and disaster recovery (consolidated 18 instances)

Health*Connect* is particularly concerned with issues of access, access restrictions and appropriate access controls. A considerable degree of attention in the Health*Connect* documentation has been focused upon ensuring an audit trail detailing every instance of access to a particular health record is retained. From a recordkeeping perspective, an audit log is an inadequate record for such purpose, being only a portion of the events that take place in the record.

Similarly, the Health*Connect* system is a complex distributed networked system, and attention to the backup and disaster recovery provisions was an expected finding. The absence of this set of functionality would have been a concern.

The major conclusions from this analysis of Parts 1 and 2 of the ISO 15489 are

- That the process of access control is the most completely articulated and detailed recordkeeping issue addressed in the business architecture.
- That the absence of details in the business architecture dealing with appropriate recordkeeping processes beyond that of access control is of significant concern.
- That the capacity to find an appropriate linkage within the Health*Connect* business architecture to the recordkeeping standards indicates that it would be possible to enhance the business architecture to encompass such concerns.

Table 6 Instances of mappings made to detailed requirements in ISO 15489.2 Records Management Standard: technical specification

ISO 15489.2 clause no.	Summary of content of section	Instances of mapping	Percentage against available 96 processes and specifications (%)
3.2	Design and implementation of records system	1	1
4.2.5.1	Access	18	19
4.2.5.2	Access	19	20
4.3.3	Registration	2	2
4.3.7.1	Disaster recovery	10	10
4.3.7.3	Backup, disaster recovery	8	8
4.3.8	Access	28	29

ISO 23081, Records management processes: metadata for records, Part 1: principles

This standard details principles on which records metadata should be designed to meet the requirements outlined in ISO 15489. The standards are therefore quite closely linked, and one would expect a degree of congruence in the mappings possible. The ISO 23081 outlines at minimum three contextual metadata entities required for appropriate record-keeping: people, business and agents and focuses on metadata created at the point of records capture as well as metadata accruing through the management processes. The conclusions of the mappings are included in Table 7.

The summary of the content of the sections indicates that a number of issues are addressed in different parts of the standard (for example, agent metadata is addressed in a number of different sections) (Table 8). If we consolidate this by issue rather than by section number, we see the clear emphasis deriving from this mapping.

These findings are consistent with the assessment of the records management standards:

- That process of access control is by far the most detailed records process defined in the business architecture and
- That attention to maintaining an audit log of transactions, particularly those relevant to access, is clearly identifiable in the business architecture.

Table 7 Instances of mappings made to detailed requirements in ISO 23081 records management processes: metadata for records

ISO 23081 clause no.	Summary of content of section	Instances of mapping	Percentage against available 96 processes and specifications (%)
8.3.3	Creating and maintaining structures for managing metadata	6	6
8.3.5	Documenting and enforcing standard definitions	6	6
8.3.6	Storage of metadata	6	6
8.3.8	Access to metadata	10	10
8.3.9	Backup, disaster recovery	2	2
8.3.9.2	Authenticity and fixity of metadata	6	6
8.4	Metadata structures	3	3
9.3.2	Creating and maintaining metadata	8	8
9.3.5	Documenting and enforcing standard definitions	6	6
9.3.9.2	Changes to metadata	8	8
9.4.2	Agent metadata: process metadata after record capture	1	1
9.5	Audit trails—fixity	26	27
9.5.1	Agent metadata	6	6
10.2.1	Agent metadata	1	1
10.3.1	Access	47	49
10.4	Agent metadata	1	1
10.5.1	Access	18	19
10.6.2	Records about records	3	3

Table 8 Consolidation of content of sections of ISO 23081 records management processes: metadata for records

Summary of content of section	Instances of mapping	Percentage against available 96 processes and specifications (%)
Access; Access to metadata	75	78
Authenticity and fixity of metadata; audit trails	43	45
Documenting and enforcing standard definitions	12	13
Agent metadata	9	9
Creating and maintaining metadata	8	8
Creating and maintaining structures for managing metadata	6	6
Storage of metadata	6	6
Metadata Structures	3	3
Backup, disaster recovery	2	2

In addition the following conclusions could be drawn:

- That the Health*Connect* business architecture adequately addresses requirements for managing metadata, metadata templates and consistent use of standard definitions.
- That the business architecture requires additional attention to metadata about agents, consistent with the emphasis on access (for identification and authentication purposes).
- That the business architecture contains less clear references to metadata about records (although this is to an extent covered in the requirements for templates defining documentary forms such as event summaries).
- That the business architecture contains no references to metadata about business processes or actions being undertaken.

Generalising from the specific findings, the conclusions of the analysis of recordkeeping standards were

- That recordkeeping processes and requirements outlined in industry standards should be far more prominent in the specification of functionality of the Health*Connect* system.
- Health*Connect* business architecture requires augmentation to include these recordkeeping processes and requirements.
- That the strong articulation of the access processes is consistent with the clear business focus of Health*Connect*, but that this is only one of the critical recordkeeping processes that need to be incorporated.
- That attention to audit and data recovery/backup reinforces the hypothesis that Health*Connect* is approaching systems design from a data management perspective that is lacking a clear incorporation of recordkeeping.
- That lack of attention to these requirements may compromise the authenticity, reliability and integrity of the Health*Connect* system.

Overall, both the quantitative and qualitative analyses found that Health*Connect*'s business architecture did not incorporate recordkeeping requirements into the business requirements to an adequate degree. There were many omissions in the system specifications in relation to the capture of records as process. The challenges of preservation and accessibility over time of the information were under presented in all Health*Connect* specifications.

Recordkeeping, legal and ethical principles and requirements for Health*Connect*

The final step in the research project was the creation of a template as a governance matrix incorporating the recordkeeping, legal and ethical principles and requirements which should guide Health*Connect*'s policies, strategies and standards and ultimately its business and systems architecture. The recordkeeping, legal and ethical principles were based on the warrants of these disciplines (laws, standards, benchmarks), and from testing the level of compliance of Health*Connect* with these principles and standards over the 3 years of the project, including the mental health case study.[6] A commentary accompanying the template documents the extent to which Health*Connect* had adhered to these principles in its final specification (Iacovino 2005).

Where there was a potential conflict between a recordkeeping, legal or ethical principle, it was identified and examined. For example, the privacy principle that requires the deletion of inaccurate personal data or the technical preservation processes that may be deemed as "further processing" that may breach privacy or personal identifiers that need to be persistently linked to the record for authenticity purposes. On the other hand, on the basis of the legal and ethical research it was decided that the fundamental right to privacy in shared health records systems must be adhered to. The template can be used to assess any cross-jurisdictional information system, bearing in mind that the replication of trust online as understood by recordkeeping models depends on a mix of policy, statutes, professional and industry standards, guidelines, and technical architectures with differing levels of compliance and enforcement due to the nature of the jurisdiction in which they are implemented (Table 9).

Although these principles should be absolute if the system is to provide reliable and authentic records that preserve patient trust, confidentiality and privacy, some compromises are inevitable. However, each principle must be taken into account in relation to the Health*Connect*'s principles and its business processes, and the risks of not adhering to them must be weighed up against the effect on patient and provider trust. Minimal requirements were reflected in the assessment of how far the business architecture conformed to recordkeeping requirements in the statistical analysis (see above).

Research outcomes

The project team produced specific outcomes in the areas of duty of care, informed consent, outsourcing, public–private organisation interaction and privacy. It derived principles for legal, ethical and recordkeeping requirements in a shared electronic health environment in the context of the last iteration of the Health*Connect* specification. These outcomes were specifically relevant to the design of the exemplar system Health*Connect* but could also be generalised to act as guidance for design criteria for other cross-jurisdictional distributed information systems. The project served as a demonstrator of the extent to which recordkeeping analysis, done using a consistent framework based on recordkeeping theory and accepted industry standards, could be constructively used to provide input to systems analysis and design. The expression of the business and the technical specification for the Health*Connect* project were sufficiently detailed to enable

[6] The governance template drew on the ARC project's Master Analysis of the 2002–2005 Health*Connect* business and systems architecture, as well as from research articles of the Chief Investigators and Research Associates.

Table 9 Extract from template of recordkeeping, legal and ethical principles and requirements for Health*Connect* 2005

Requirement and principle			Health*Connect* principles and example processes (BA v1.9 2004)	Recordkeeping, legal and ethical warrants
Recordkeeping	Law	Ethics		
Ensure patient and provider identifiers accurately identify individuals • Verify the identity of the consumer/patient and providers against identifier • Ensure that the personal data that is linked to the identifier are accurate and protected from disclosure • Ensure that consumer and provider updates are notified to the HRS • Adopt identification and authentication methods that protect the identity of the sender and recipient Principle Authentication of individuals involves managing personal information that forms part of the identity of a record transaction See also Define and implement access privileges for consumers and providers Consent	Ensure statutory penalties are appropriate for the misuse of identifiers Principle Data accuracy is a privacy principle endorsed internationally and found in all Australian privacy legislation Correct identification of persons in relation to health data is essential. Limit linkages that have not been expressly consented to by the patient	Minimise potential harm caused by misuse of identifiers Principle Respect privacy via the ethical principle of autonomy Record linkages undermine patient autonomy if the patient has not consented to the linkage	*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* (HC Principle, BA v1.9, p. 30) Processes from registration agency perspective: C4.5.3 Consumer registration requirements–consumer registration service C4.6.3 Provider registration requirements–provider registration service C-164 Health*Connect* solutions should be prepared to adopt the national health identifier as the authoritative source of unique consumer identification for Health*Connect*, when the identifier becomes available C-168 When and if it becomes available, a national health provider identifier should be adopted by Health*Connect* solutions as the authoritative source of unique provider identification for Health*Connect*.	Recordkeeping Interpares 1 2001 benchmark requirements for assessing the authenticity of electronic records, A6 Authentication of records: if authentication is required by the juridical system or the needs of the organisation, the creator has established specific rules regarding which records must be authenticated, by whom, and the means of authentication Confirmation of identity: AS 5017—2002 health care client identification Section 5: data matching AS 4590—1999 interchange of client information Legislation and codes Electronic Transaction Acts re-authentication; Evidence Acts (federal and state); Health Records Acts, e.g. HPP 15 of the *Health Records and Information Privacy Act* 2002 (NSW) specifically covers an individual's express consent to the use of his or her identifier for record linkages Draft National Health Privacy Code NHPP 7 Identifiers Ethics Bioethics and principle of patient autonomy. This principle states that it is up to the patient to decide who should have access to his/her personal health information

identification and location of the records implicit in the specifications. From there, it was possible to identify record ownership, custody, authenticity and accessibility issues and provide a coherent analysis of record requirements relevant to their creation, management and retention. Thus, the research tools in themselves were a significant outcome, as were the new interdisciplinary collaboration and understandings within the multi-disciplinary research team. In particular the recordkeeping tools did not stand alone but incorporated the legal and ethical analyses.

The research also produced a set of findings and recommendations drawn from the analyses of the policy documents, and the business and technical architecture aimed at legal strategists, policy makers, clinicians, medical records managers and informatics professionals. The recommendations were disseminated during the course of the research project in interdisciplinary scholarly journals, especially legal, medical and health information management, through government submissions, legal and health information conferences, a national symposium organised by the research team dedicated to Health*Connect*, and an international forum in order to influence policy and systems development and inform legal and health professionals of the impact of Australian shared health records' initiatives on their work practices.[7] The dissemination of project outcomes at the national and international level was consciously designed to communicate to broad communities of practice beyond individual disciplines.

The outcome of the recordkeeping analysis of the Health*Connect* specifications identified many specific findings aimed at improving the compliance of Health*Connect* to recordkeeping benchmarks. Broadly speaking, the findings can be summarised into the following areas:

Governance

The research found that Health*Connect*'s lack of a finalised governance structure impacted on all aspects of the project but was particularly significant in relation to ownership issues and records retention. Ownership of Health*Connect* records in the different layers of the architecture must be clarified in order to resolve questions of record control and ownership. Jurisdictional questions must be clarified in the long term, even if in the short term by default the records seem to reside in the federal arena. To ensure adequate legislative protections operating over the federated HRS, the Health*Connect* governing body should be a cross-jurisdictional authority.

Long-term retention

The research found that the life cycle model of systems analysis underpinning the development of the Health*Connect* architecture proved inadequate to address the significant concerns raised by the intention to manage a longitudinal health record, i.e. a health

[7] The results of the recordkeeping, privacy and ethical analyses as on April 2004 were published in J Law Med (2004) 12(1), Special Issue on Electronic Health Records, following a National Symposium organised by the ARC project team: Shared Electronic Health Records: Ethical, Legal and Recordkeeping Perspectives, School of Law, Deakin University, Melbourne, 23 April 2004; findings as on September 2005 were presented at an International Workshop: The Long-term Curation and Preservation of Medical Databases, Digital Curation Centre, University of Glasgow and Electronic Resource Preservation and Access Network (ERPANET), Calouste Gulbenkian Foundation, Lisbon, Portugal, 13–14 October 2005. Research findings on privacy and confidentiality, in particular secondary uses of Health*Connect* data, have been published in Iacovino (2006).

record which has an inbuilt assumption of long-term retention for at least the life of a patient. The issues of preservation, given the aim of the system to present a reliable longitudinal record, will significantly affect the reliability and authenticity of the record. Health*Connect* requires a clear statement on which digital preservation strategies to adopt, and where, in the complex array of repositories, the responsibility for preservation over time will occur. Depending upon the articulation of the ownership issues and clear identification of responsibility for records at each layer of the architecture, different bodies potentially under different jurisdictional rules will assume preservation responsibility. This responsibility should be clear from the design stage of the project. Of course, the political complexity of multiple jurisdictions and the lack of clear articulation of governance for the Health*Connect* system impede development of this clarity; however, reliability and authenticity, and consequently trust in the system will be severely compromised without it. The notion of trusted third parties who could store distributed records was not addressed (Iacovino 2004a).

Inappropriate reliance on audit trails as a recordkeeping technique

Health*Connect*'s business and technical specifications use understandings from the information systems community revealing a lack of understanding of recordkeeping requirements. For a health *records* system, this is an ironic finding. Thus, the assumption that maintaining audit trails is an appropriate recordkeeping technique was embedded in later versions of the specification to address requirements to be able to trace changes and uses of the data. Audit trails as recordkeeping tools may address changes to the data but will always fail to maintain persistent linkage to other information (for example, provider registration details) required to interpret the record over time.

The use of audit trails as recordkeeping tools was specified in relation to access interactions with the health records, but lacking for other processes important to prove assurance to assertions of authenticity, reliability and integrity of the record. Statements requiring the replication of audit trail data to the NDS as the repository for long-term data are insufficiently granular to be practical. Not all audit trail data (or in records terms, recordkeeping process metadata) will need to be retained forever, but the absence of a coherent recordkeeping framework for analysis in the design of the specifications makes the differentiation between what needs to be retained in the long term and what can be disposed of difficult, with the consequence of a default position of keeping all specified audit data. The research team hypothesised that this will become an undue burden to the system and will be unlikely to be implemented, causing potential compromise of authenticity of the records.

Recordkeeping as a process

Archiving must be a part of every process at all times and places as it affects the formation of the record. How the record is defined, i.e. whether it includes context (process and transaction metadata in addition to metadata about the document structure and schema) or just content, affects the record's long-term preservation and accessibility. The Health*Connect* conceptualisation of record was focused on the object (the SEHR), but it failed to appreciate requirements to ensure process records associated with the individual object to maintain authenticity, reliability and integrity of the record, both for its immediate requirements and to meet the long-term preservation intentions expressed in Health*Connect*'s own data principles.

The recordkeeping analysis found that the SEHR is a conceptual rather than a physical entity. The SEHR 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 SEHR. To adequately protect authenticity, integrity and reliability of the SEHR, each of these processes needed to be considered from a recordkeeping perspective. Attempting to address recordkeeping issues (such as retention and disposal or access) from a one-dimensional view of the SEHR as an object is not appropriate to the project design or to the conceptual models or recordkeeping as advocated by best practice industry standards. Additional services that stand outside the HRS also create records that relate to the SEHR, for example, registration records. The object view of a record does not provide a definable logical boundary that can be linked to a responsible person. Therefore, defining the record as process had been necessary to capture all the activities that created records (Reed 2005a).

Dynamic records

The Health*Connect* specifications did not sufficiently address the dynamic nature of the SEHR. Replication of data between layers in the technical architecture will not create complete copies, as the functionality of each layer continues to accumulate process metadata about the management and use of the data specific to each layer. Issues of synchronisation and managing multiple versions of the record at different layers will be simplified by conceptualising a number of different records, each valid for different purposes, held by different parts of the architecture. Similarly, exploration of reliability of the SEHR content given the availability of patient participation in maintaining the content of the record has not been afforded sufficient attention in the design specification (Iacovino 2004a).

Managing views of the data as record

Access to SEHR data is through the use of tailored views of the aggregated data accumulating on one individual. The data that is presented to an authorised user, whether a clinician providing point of service care, or a secondary user, must be retained as a record in its own right, particularly for clinicians, as this is the data on which decisions are made. The system specifications are very vague on recordkeeping for this critical data, depending on the ability to replicate data presented at a specific time, using standardised lists and views. This approach fails to take into account the potentially dynamic nature of the record with updates and changes, contributed at various times by various parties. Responsibility for maintaining this record may well lie with the querying clinician, but the specification is silent on requirements for incorporating this into the point of care systems.

Other areas of the research project undertook extensive analysis of the consent models and their adequacy to meet essential privacy concerns. As indicated earlier the consent models were simplified with every iteration of the specification, leaving an inadequate model, whereby express consent was required only for the initial sign up and implied once the patient was in the system. The use of a “standing consent” until one opts out has been accepted. Recordkeeping requirements managing consent and matching authenticated access rights to records will be needed, but have not been developed while the consent models are in flux. Indeed the complexities of managing such contextually sensitive records over time may have been instrumental in the simplification to a technically implementable model, but one which fails to address significant community and contributor concerns.

Conclusion

Using Health*Connect* as a working exemplar, the project analysed the roles and responsibilities of participants, the complex issues of ownership, location and records transactionality. These issues are critical to patients' and health providers' rights and responsibilities, and long-term viability of such systems. The ability to ensure trust in the systems is a critical component affecting voluntary uptake of systems of this kind as a means of doing business. The project analysed redesigned business processes to support the delivery of electronic health outcomes to ensure that the authoritative recordkeeping issues critical to authenticity and trust in such systems can be addressed. The project also enabled exploration of means of communicating such issues and concerns from a multi-disciplinary perspective beyond those dictated by the immediate business drivers in design phases of complex distributed and networked systems. In doing so, the project demonstrated how the issues could be incorporated into design, a critical factor in social acceptance, community trust and ongoing viability of such systems. This provides significant potential economic benefits in incorporating mechanisms to address the issues in the system design rather than having to patch or redesign the system operation as the issues of concern are revealed after the system is operational. The team's recommendations if implemented would have reduced the risks that such a system might otherwise pose to the doctor–patient relationship and to the security, authenticity or integrity of health records.

The tools and techniques used to conduct the recordkeeping research in this project included adoption of an external conceptual framework—the records continuum model; recordkeeping benchmarks; the recordkeeping standards and prior research project outcomes and the development of analytic tools using business analysis documentation, metadata mapping techniques, statistical analysis and governance matrices. These tools and techniques were applied to a single instance of an emerging large-scale, cross-organisational electronic transaction system. The research team proposes that these tools and techniques will be able to be applied to other such systems. To that end, the project outcomes were consciously formulated in ways that will be able to inform design and development of future projects involving cross-jurisdictional electronic transaction-based systems.

Although at the conclusion of the research project implementation of Health*Connect* had been put on hold, a new governance structure for such a system and a national health card with personal health information remained on the government agenda, indicating that issues identified by the project remain relevant to shared networked health systems (Consumer and Privacy Taskforce 2006). In fact, the Health*Connect* policy changes validated the research findings of the project, in particular the critical role of governance arrangements.

Of equal importance to the findings and recommendations, the project team developed expertise in methods of appropriate communication of the issues with disparate information and professional communities with multiple different agendas. The innovation in cross-disciplinary collaboration was of itself a significant outcome. The successful conclusion of the project sets a strong precedent for continuing multi-disciplinary collaboration, particularly in the design and development of cross-jurisdictional networked transaction-based systems into the future. From a continuum perspective, the project demonstrates that archivists must be involved in record formative processes to ensure that records are captured and preserved, well before they are under archival control.

Acknowledgements The authors would like to acknowledge Australian Research Council (ARC) Discovery Grant, 2002–2005 for funding the project *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework* and also acknowledge the Chief Investigators: Associate Professor Danuta Mendelson, School of Law, Deakin University; Dr. Livia Iacovino, School of Information Management and Systems (Caulfield School of Information Technology), Monash University; Professor Bernadette McSherry and Dr. Moira Paterson, Faculty of Law, Monash University; Research Associates Barbara Reed (2002–2005), Hans Hofman (2004–part 2005), Robert Meredith (2003) and Angela Randall (2003) for their support.

References

Consumer and Privacy Taskforce (2006) Health and social services: access card, report number one, September 2006. Australian Government, Department of Human Services, Canberra. http://pandora.nla.gov.au/pan/65938/20070207-0000/www.accesscard.gov.au/various/Consumer_privacy_rp2.pdf. Consulted July 2008

Health*Connect* (2002a) Draft Health*Connect* business architecture v0.7, March 2002. Department of Health and Ageing, Canberra. http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/2FD500E405B5576DCA257128007B7EAC/$File/ba07_com.pdf. Consulted July 2008

Health*Connect* (2002b) Health*Connect* project overview, September 2002. Department of Health and Ageing, Canberra. http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/BA6DCE09CA000739CA257128007B7EB1/$File/projovw.pdf. Consulted July 2008

Health*Connect* (2003a) Draft systems architecture, architecture overview draft v0.9, July 2003. Department of Health and Ageing, Canberra. http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/2FD500E405B5576DCA257128007B7EAC/$File/sao1-60.pdf. Consulted July 2008

Health*Connect* (2003b) Interim research report, volume 1. Overview and findings. Department of Health and Ageing, Canberra. http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/43598FE37A3E7270CA257128007B7EB7/$File/v1.pdf. Consulted July 2008

Health*Connect* (2003c) Interim research report, volume 2. Research reports, research report 5, what will be necessary to manage privacy? April 2003. Department of Health and Ageing, Canberra. http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/43598FE37A3E7270CA257128007B7EB7/$File/v2-5.pdf. Consulted July 2008

Health*Connect* (2003d) Interim research report, volume 3. Background documents part 6: Health*Connect* business architecture v1.0, July 2003. Department of Health and Ageing, Canberra. http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/43598FE37A3E7270CA257128007B7EB7/$File/v3-6.pdf. Consulted July 2008

Health*Connect* (2004a) Business architecture v1.9, version for comment, November 2004. Department of Health and Ageing, Canberra. http://www.healthconnect.gov.au/pdf/BArc1-9.pdf. Consulted November 2005

Health*Connect* (2004b) Business architecture v1.9, version for comment. Specification of Health*Connect* business requirements, November 2004. Department of Health and Ageing Canberra. http://www.healthconnect.gov.au/pdf/BAV1-9g%20Attach.pdf. Consulted November 2005

Health*Connect* (2008) Overview of Health*Connect*. Department of Health and Ageing, Canberra. http://www.health.gov.au/healthconnect. Consulted July 2008

Hofman H (2005) Preliminary analysis of dataflows in the Health*Connect* system, April 2005. Report for, electronic health records: achieving an effective and ethical legal and recordkeeping framework. Australian Research Council Discovery Grant, 2002-05, School of Law Deakin University, School of Information Management and Systems Faculty of Information Technology, and Faculty of Law Monash University, Australia. http://infotech.monash.edu.au/research/centres/cosi/projects/arc-report1.pdf. Consulted July 2008

Iacovino L (2003) A recordkeeping critique of shared electronic health records: a preliminary analysis of the Australian Research Council, Discovery Grant, Electronic health records: achieving an effective and ethical legal and recordkeeping framework. In: McCarthy R (ed) Proceedings, 24th health information management association of Australia conference, Sydney, 8–10 August 2003, HIMAA, Sydney (n.p)

Iacovino L (2004a) Trustworthy shared electronic health records: recordkeeping requirements and Health*Connect*. J Law Med 12(1):40–59. doi:10.1093/medlaw/12.1.40

Iacovino L (2004b) The patient-therapist relationship: reliable and authentic mental health records in a shared electronic environment. Psychiatry Psychol Law 11(1):63–72

Iacovino L (2005) Recordkeeping, legal and ethical principles and requirements for Health*Connect*. Report for, electronic health records: achieving an effective and ethical legal and recordkeeping framework. Australian Research Council Discovery Grant, 2002-05, School of Law Deakin University, School of Information Management and Systems Faculty of Information Technology, and Faculty of Law Monash University, Australia. http://infotech.monash.edu.au/research/centres/cosi/projects/arc-report2.pdf. Consulted July 2008

Iacovino L (2006) Beyond the tomb: privacy, confidentiality, and long-term preservation of and access to electronic health records in national systems a case study of Australia's Health*Connect* project. Arch Manuscr 34:10–39

Iacovino L, Mendelson D, Paterson M (2006) Privacy issues, Health*Connect* and beyond. In: Freckelton I, Petersen K (eds) Disputes and dilemmas in health law. The Federation Press, Sydney, pp 604–621

Ingram D (2002) The origins of openEHR. OpenEHR Foundation. http://www.openehr.org/about/origins.html. Consulted July 2008

InterPARES 1 Project (2001) Authenticity task force, final report, 28 October 2001. University of British Columbia, Vancouver. http://www.interpares.org/documents/atf_draft_final_report.pdf. Consulted July 2008

ISO/TC 215 (2002) Standards requirements for the electronic health record and discharge/referral plans. Ad hoc group report, Draft V 2.1, 31 May 2002

ISO/TC 215 (2003) Electronic health record definition, scope, and context. Technical report. Draft V0.1, First Draft, 7 July 2003

Kearsey I (1989) Some problems in placing modern medical records in public archives. Arch Manuscr 17(2):183–196

MacNeil H (2005) Information privacy, liberty, and democracy. In: Behrnd-Klodt ML, Wosh PJ (eds) Privacy and confidentiality perspectives: archivists and archival records. Society of American Archivists, Chicago, pp 67–81

McSherry B (2004a) Ethical issues in Health*Connect*'s shared electronic health record system. J Law Med 12(1):60–68

McSherry B (2004b) Third party access to shared electronic mental health records: ethical issues. Psychiatry Psychol Law 11(1):53–62

Mendelson D (2003) Travels of a medical record and the myth of privacy. J Law Med 11(2):136–145

Mendelson D (2004) Health*Connect* and the duty of care: a dilemma for medical practitioners. J Law Med 12(1):69–80

Meredith R (2004) VERS—openEHR mapping commentary: a mapping of the Victorian Electronic Records Strategy Schema to openEHR January 2004 for, electronic health records: achieving an effective and ethical legal and recordkeeping framework. Australian Research Council Discovery Grant, 2002-05. School of Law Deakin University, School of Information Management and Systems, Faculty of Information Technology, and Faculty of Law, Monash University, Australia. http://infotech.monash.edu.au/research/centres/cosi/projects/arc-report5.pdf. Consulted July 2008

Monash University, School of Information Management Systems (1999) Recordkeeping metadata standards for managing and accessing information resources in networked environments over time for government, social and cultural purposes. Monash University. http://www.sims.monash.edu.au/research/rcrg/research/spirt/index.html. Consulted July 2008

National Electronic Health Records Taskforce (2000) A health information network for Australia taskforce report. Department of Health and Aged Care, Canberra

National E-Health Transition Authority (2007) Annual report 2006-07. Sydney, New South Wales. http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=-1&Itemid=139. Consulted November 2007

Paterson M (2004) Health*Connect* and privacy: a policy conundrum. J Law Med 12(1):80–90

Paterson M, Iacovino L (2004) Health privacy: the draft Australian national health privacy code and the shared longitudinal electronic health record. Health Inf Manag J 33:5–11

Public Record Office Victoria (1998) Victorian electronic records strategy, final report. Public Record Office Victoria. http://www.prov.vic.gov.au/vers/pdf/final.pdf. Consulted July 2008

Reed B (2004) Accountability in a shared services world. Paper presented at the Australian Government Information Management Office and Institute of Public Administration ACT Division, Australia Future Challenges for E-Government, Canberra, May 2004

Reed B (2005a) Issues arising from analysis of the Health*Connect* business architecture v1.9, July 2005. Report for, electronic health records: achieving an effective and ethical legal and recordkeeping framework. Australian Research Council Discovery Grant, 2002-05. School of Law Deakin University, School of Information Management and Systems Faculty of Information Technology, and Faculty of Law Monash University, Australia. http://infotech.monash.edu.au/research/centres/cosi/projects/arc-report4.pdf. Consulted July 2008

Reed B (2005b) Recordkeeping standards analysis June 2005. Report for, electronic health records: achieving an effective and ethical legal and recordkeeping framework. Australian Research Council Discovery Grant, 2002-05. School of Law Deakin University, School of Information Management and Systems Faculty of Information Technology, and Faculty of Law Monash University, Australia. http://infotech.monash.edu.au/research/centres/cosi/projects/arc-report3.pdf. Consulted July 2008

Rooney T, Aitken J (2002) Health*Connect*, consent and electronic health records: a discussion paper, July 2002. Health*Connect* Program Office, Canberra. http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/E250BD83358D3A56CA257128007B7EC9/$File/cons_dp.pdf. Consulted July 2008

Terry NP (2004) Electronic health records: international, structural and legal perspectives. J Law Med 12(1):26–39

Author Biographies

Dr. Livia Iacovino is an Honorary Senior Research Fellow with the Centre for Organisational and Social Informatics in the Faculty of Information Technology, Monash University, Australia, where she has taught the legal and ethical curricula in the recordkeeping courses. Her research and publications are focused on interdisciplinary perspectives of archival science, law and ethics, in particular ownership, access and privacy of electronic records. She has been a Chief Investigator for Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework, an Australian Research Council Discovery Grant and has collaborated internationally with the InterPARES Project and the International Records Management Trust.

Barbara Reed has been involved with industry, teaching, research and standards setting, in the course of her 25 years in the recordkeeping and information management communities. She has been the Director of The Recordkeeping Institute since 2000 and has over 20 years consulting experience to all levels of government, private and public companies and not-for profit organisations. She has developed and negotiated Standards for recordkeeping at state, national and international levels. She has published widely on metadata definition and deployment, recordkeeping, interoperability, management of resources over time and digital preservation. She was a Research Associate in the Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework, 2002–2005, and Clever Recordkeeping Metadata, 2005–2006, both ARC Projects.