Recordkeeping, Legal and Ethical Principles and Requirements for HealthConnect: Template V1.0

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

Livia Iacovino  
Caulfield School of Information Technology  
Monash University  

July 2005/Amended July 2008
Introduction

The recordkeeping, legal and ethics principles in this governance template are based on the ‘warrants’ of these disciplines. Potential conflicts between recordkeeping principles and legal or ethical ones have been noted, for example, the privacy principle that requires the deletion of inaccurate personal data, personal identifiers that need to be persistently linked to the record for authenticity purposes, and technical preservation processes that may be deemed as ‘further processing’ that may breach privacy. On the other hand, there are strong arguments for insisting that the fundamental right to privacy should be adhered to in shared health records systems. In practice, many of the issues with the management of personal data contained in records can be mitigated by anonymisation, encoding and processing conditional upon procedures followed by either the data controllers or researchers.1

Although the template 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 HealthConnect principles and its business processes, and the risks of not adhering to them must be weighed up against the affect on patient and provider trust.

The extent to which HealthConnect has adhered to these principles, and more specifically recordkeeping requirements and standards, is summarised in the template below. The template and commentary are drawn from the Master Analysis of the 2002-2004 versions of the business and systems architecture which provides a more detailed analysis of the recordkeeping requirements and standards; principally ISO 15489, International Standard on Records Management, Parts 1 and 2-2002; ISO 23081, Records Management Processes–Metadata for Records, Part 1–Principles-2005; InterPARES 1 Project, “Requirements for Assessing and Maintaining the Authenticity of Electronic Records”, 2001, and the InterPARES 1, Principles of the Strategies Task Force Report, as well as from research papers and presentations of the research project. In addition the Pittsburgh requirements have been noted where they express an additional feature not found explicitly in the records management standard.

---

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Define record as process and capture all processes as records</td>
<td>Recognise record as process rather than as object in evidence law</td>
<td>Maintain control over personal data for patient autonomy through ownership of process</td>
<td>Where access to an HRS (such as a query) results in new artefacts being added to an EHR, those artefacts will form part of the updated EHR material that the HRS supplies to the National Data Store. (BA 1.9 p. 113.)</td>
<td>Recordkeeping</td>
</tr>
<tr>
<td>• Maintain a process record of what has changed, who did it, time when event summary is updated</td>
<td>Principle The best evidence rule, that is, the production of an original record is the best evidence defines electronic records as products of processes.</td>
<td>Ethical principle of autonomy</td>
<td>Example processes. Process G3 - Retrieve/use EHR Information</td>
<td>ISO 15489.1, 3.15 Records and 7.2.1 Characteristics of a record-General.</td>
</tr>
<tr>
<td>• Ensure that every access creates a record of the recordkeeping transaction: date, what accessed, who, when</td>
<td>Legal ownership of process</td>
<td></td>
<td>Process J2 - Provide EHR View/List</td>
<td>ISO 15489.1: 8.3.2 Documenting records transactions: Records systems should contain complete and accurate representations of all transactions that occur in relation to a particular record</td>
</tr>
<tr>
<td>• Changes to consumer EHR and source of change recorded in</td>
<td>Evidence of access and misuse of data</td>
<td></td>
<td>Process J3 - Process EHR Query/Response</td>
<td>ISO 23081 10.6.2 Process metadata about records management processes after record capture: Creating metadata about records management processes is an essential component for assuring the authenticity, integrity, usability and reliability of records.</td>
</tr>
</tbody>
</table>

Livia Iacovino: Recordkeeping, Legal and Ethical Principles and Requirements for HealthConnect: Template V1.0
July 2005
### Principle: Record authenticity

- Record characteristics

- Implement if material is registered in the records system prior to forwarding to the designated persons.

### Legislation

**Evidence Act 1995 (Cth) ss 146 and 147.**

### Ethics

**Bioethics and principle of patient autonomy.**

---

### Recognise that preservation of authentic records is a continuous process requiring active intervention

- Protect health records from accidental or intended damage or modification, in particular due to hardware and software obsolescence.
- Use digital

### Recognise that evidence law allows for electronic documents to be admitted into legal proceedings, including authentic copies as “originals”

**Principle**

The best evidence rule, that is, the production of an original record is the best evidence. Electronic records as processes in evidence law.

### Minimise the harm that may result to a patient or provider if reliable and authentic records are not preserved over time

**Principle**

Utilitarian principle in bioethics on minimisation of harm to patient.

### HealthConnect will be a repository service for consumers’ lifetime health records. (BA v1.9 p. 37) and EHR data will be permanently recorded and preserved subject to legal constraints. (BA v1.9 p. 34.)

- The *HealthConnect data model must be extensible to accommodate evolution of the content and format of EHR information over time.* (BA v1.9 p. 34.)
- *HealthConnect data structure, systems and processes must be designed to maintain backward compatibility and integrity of the stored data so that can only be effectively implemented if material is registered in the records system prior to forwarding to the designated persons.*

### Recordkeeping

**ISO 15489.2 4.3.7.1 Risk management also involves development of a disaster recovery plan ...**

- **ISO 23081 8.3.9 Maintenance of metadata: Processes and methods: d) backup procedures**
- **ISO 15489.2 4.3.7.1 For electronic records, use of reliable systems and media that have greater and more robust life spans will be indicated.**
- **ISO 15489.2 4.3.7.3 Digital storage: a) backup systems are a method of copying electronic records to prevent the loss of**
<table>
<thead>
<tr>
<th>Signatures to safeguard record integrity both at the time the transaction takes place as well as once it is archived.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that records can be read in an unencrypted form, with appropriate contextual information.</td>
</tr>
<tr>
<td>Put into place procedures and systems that allow the capture and maintenance of recordkeeping metadata that documents the validation of a digital signature and the encryption of a record.</td>
</tr>
<tr>
<td>Produce documentation to prove the</td>
</tr>
<tr>
<td>Process Examples: B9-C-75 Coordinate HealthConnect records management functions, (d) management of data loss, and data recovery; ... Process I5 - Maintain compatibility with HealthConnect metadata. ... to ensure that incoming EHR information using updated formats is not lost.</td>
</tr>
<tr>
<td>Process I6 - Maintain HRS processing platform and network environment.</td>
</tr>
<tr>
<td>C-166 HealthConnect solutions should adopt harmonised international EHR standards as these are developed and should apply them in the interchange and interpretation of HealthConnect event summaries, lists and views.</td>
</tr>
<tr>
<td>records through system failures.</td>
</tr>
<tr>
<td>Interpares A8: Removal and Transfer of Relevant Documentation.</td>
</tr>
<tr>
<td>Data format standards and protocols eg XML (eXtensible Markup Language).</td>
</tr>
<tr>
<td>National Archives of Australia, Recordkeeping and Online Authentication and Encryption, Archives Advice 64, Issued September 2003 /Revised May 2004</td>
</tr>
<tr>
<td>National Archives of Australia, Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption, May 2004</td>
</tr>
<tr>
<td>National Archives of Australia, DIRKS: A Strategic Approach to Managing Business Information, Archives Advice 51, August 2001</td>
</tr>
</tbody>
</table>


*Evidence Act 1995 (Cth)* ss 146 and 147.

*Electronic Transactions Act 1999*

*Archives Act 1983*

*Freedom of Information Act 1982*

*Privacy Act 1988.*

**Ethics**

National Health and Medical Research Council Act 1992, s 8, Ethics Guidelines

National Health and Medical Research Council, *National...*
| Comply with laws of the relevant jurisdiction | Ensure records have the capacity to be used as legal evidence | Recognise that ethical duties require clear allocation of responsibilities to persons (juridical and natural) | HealthConnect is a cooperative venture between the Australian State and Territory Governments to implement a national EHR solution which will operate seamlessly and consistently across Australia, with the same rules for privacy, identification, registration and consent applying everywhere (BA v1.9 p. 24).

B 8 Complaints Process Process B8 - Handle consumer and provider complaints.

See processes dealing with registration, identification, and consent. | Recordkeeping ISO 15489-1, 5. Regulatory environment. ISO 23081, 10.3.1 Metadata about the business rules, policies and mandates at point of records capture: ...metadata should document records compliance with business rules and policies, regulatory and other requirements for creating and managing records...a) identify the specific metadata scheme or schema used in organisational business systems b) capture the business rules or other system controls that regulate record creation and management c) capture the business rules or other system controls that regulate metadata creation and management...e) capture the business rules or other system controls that regulate access and rights to records f) document the mandate or other regulatory requirement for |

**Principle**

Record compliance

- Create and capture records that are either implicitly or explicitly required by the legal system.
Pittsburgh (1) Compliant: Organizations must comply with the legal and administrative requirements within the jurisdictions in which they operate, ...

Interpares A5: The creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator.

**Law**
Limits of federal power over medical practice. *Constitution Act 1900 Cth*, s 51(xxiiiA).

Medical Practice Acts
Evidence Acts
Health Act
Privacy Acts
FOI Acts

**Ethics**
Deontological duties. Legal or moral consequences of non-documentation including sanctions and penalties.
**Capture reliable and accurate records at each level of the HealthConnect architecture**

- Register each record in the system uniquely
- Undertake quality rating on the reliability of the information coming from patients.
- Document the sources of the data.
- Place controls over update processes.
- Ensure that providers are using the most recent/up to date records.
- Synchronise the HRS with the local practice systems.

**Recognise the legal implications of relying on incomplete records (eg evidence and ‘weight’)**

**Principle**
Provider liability and indemnity re: accurate/inaccurate shared health records.

A medical practitioner has a legal duty to create an accurate record at the time of each professional encounter with the patient.

Patient has a duty to tell the truth to the practitioner (not a true legal duty but could be used by a practitioner as a defence).

**Recognise the ethical implications of relying on incomplete records**

**Principle**
A medical practitioner has an ethical duty to create a record at the time of each professional encounter with the patient.

Patient has an ethical duty (deontological) to tell the truth to the practitioner.

**Each entry in a consumer’s HealthConnect EHR must be attributed to an individual provider, on behalf of an authorised provider organisation, the consumer or another person authorised to add information to the EHR.**

HealthConnect will promote a focus on data quality checking in source systems.

Consumers will have access to HealthConnect to view and, in the future, contribute to their EHR information.

Consumers, at the time of a consultation, may request personal information to be withheld from HealthConnect. The provider will, on request, not send the event summary or delete the information prior to sending the event summary.

**Recordkeeping**
ISO 15489, the International Standard on Records Management 7.2.2-7.2.5. “Reliability”.

ISO 15489.1: 9.2 Determining documents to be captured into a records system.

ISO 15489.1 9.4: The primary purpose of registration is to provide evidence that a record has been created or captured in a records system, and an additional benefit is that it facilitates retrieval. It involves recording brief descriptive information or metadata about the record and assigning the record an identifier, unique within the system.

ISO 15489.2, 4.3.3 Registration: Whatever form it takes, as a general rule the register is unalterable. If, however, changes are required, there has to be an audit trail.

Interpares A5: Establishment of documentary forms: the creator has established the documentary forms of records associated with each procedure according to the requirements.
| Principle | Record reliability | available as soon as possible after a health event and hence, as far as practicable, should be submitted directly following the completion of an event. (BA v1.9 p. 33.)

HealthConnect will not perform any clinical validation of the data in the event summary. (BA v1.9 p. 33.)

Process examples.
Process E4 - Send/receive eHealth communication.
Process K1 - Validate incoming event summary
C-146 Process Event Summary and Update EHR
C-144 and C-145... the following formats.
C-166 HealthConnect solutions should adopt harmonised international EHR standards

of the juridical system or those of the creator

Interpares A1b.iii (Integrity of the record). Indication of types of annotations added to the record

ISO 23081.1 9.3.5
Documenting and enforcing standard definitions: Agents, including records managers, should document the rules and policies on consistent use of content standards, structures, terms and other related, relevant issues. They should ensure that those metadata structures, terms, entity descriptions and attributes are used in a consistent way.

Pittsburgh (5) Comprehensive: Records must be created for all business transactions.

Agreed messaging standards improve reliability. See HL7 transmission protocols

Legislation
Recordkeeping processes and systems need to be shown to have operated consistently and reliably as part of the normal course of a business to satisfy legal evidence, for example *Evidence Act 1995 (Cth)* ss146 and s 147.

The Medical Practice Regulations, 1998 (NSW), Reg. 13, 14(1), and 15(1) specify that a record for each patient must be made and kept by a medical practitioner, when it should be made, and how long it needs to be kept, and Schedule 2 prescribes what details the record must contain about the patient.

**Ethics**

Duties of practitioners and patients, for example the Australian Medical Association Code of Practice.

| Capture authentic records at all levels of the HealthConnect architecture | Recognise the legal implications of relying on records that have been altered or cannot be correctly identified (eg evidence and information, once submitted to HealthConnect, may not be deleted or altered; however corrections or amended information may be included in the EHR by issuing revised versions of the information) | Recognise the ethical implications of relying on records that have been altered or cannot be correctly identified | Recordkeeping ISO 15489, the International Standard on Records Management 7.2.2-7.2.5. “Authenticity” and “Integrity”. ISO 15489.1: 7.4.2 Integrity: |

Livia Iacovino: Recordkeeping, Legal and Ethical Principles and Requirements for HealthConnect: Template V1.0

July 2005
- Ensure that patient amendment rights do not diminish a record's integrity.
- Ensure synchronisation between HRS, CIS and NDS.
- Ensure that each record at each layer of HealthConnect captures the context in which it is created.
- Ensure security of transmission of event summary to HRS and its subsequent integrity.
- Ensure security of transmission of event summary to admissibility).

### Principle

**Medical duty to advise/warn patient, and which records the courts would rely on as the “full and accurate” record.**

To reconstruct what a clinician saw when treating a patient requires the preservation of all the data on which a medical decision is based, including the summary record.

Evidence law requires evidence of a record's provenance.

### Principle

**Ethical intentions are evidenced by outcome, therefore evidence of intention or at least circumstantial evidence of intention is essential to ethical action.**

*All changes to the consumers EHR data must be versioned and retained on the audit trail in such a way that previous versions of EHR information can be accessed. (BA v1.9 p. 142.)*

*Each consumer will be registered in one HRS. A copy will be transmitted to the National Data Store for archiving and long term retention. (BA v1.9 p. 7)*

*Examples of related processes: Process E3 - Update consumer EHR information. A key aspect of the definition of views will be the maintenance of the integrity of the information presented in the view and ensuring that important components of an EHR are always included so that information cannot be misinterpreted by being seen out of context. (BA v1.9 p. 44)*

*Process I7 - Apply and monitor ICT security measures. Each AEM will be responsible for the*
NDS and its subsequent integrity

- Ensure security of transmission of event summary to CIS and its subsequent integrity
- Need to show that the system consistently captures the view and related metadata.

**Principle**

Authenticity is not compatible with anonymisation unless it is reversible.

**See also** identity, integrity, record as process and audit trails.

security and access control of EHR information held in the HRS that they own and operate. C-136. Each AEM must protect the confidentiality, integrity and availability of the consumer’s HealthConnect EHR information.

Providers will continue to maintain their own consumer health records but may choose to incorporate selected HealthConnect EHR information in their records or clinical information systems. (BA v1.9 p. 29.)

Once HealthConnect EHR information has been entered into a local system, the owner of that system has responsibility for the security of the information. (BA v1.9 p. 77.)

effective controls to guarantee the records' identity and integrity. Integrity during and after transmission

AS 4846 – 2004, Australian Standard for Health Care Provider Identification

ISO 23081 10.2.1 Metadata about records at point of record capture: …metadata about the record should b) identify and describe the persons involved in records creation

National Archives of Australia, Recordkeeping Metadata Standard for Commonwealth Agencies, Archives Advice 41, Issued April 2000/Revised August 2000

Interpares A8 Removal and Transfer of Relevant Documentation: if there is a transition of records [from active status to semi active and inactive status] which involves the removal of records from the electronic system, the creator has established and effectively implemented procedures determining what
documentation has to be removed and transferred to the preserver along with the records.

Interpares 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.

Interpares A7: Identification of Authoritative Record: If multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative.

Interpares B1 Controls over records transfer, maintenance and reproduction: The procedures and systems used to transfer records to the archival institution or program, maintain them, and reproduce them embody adequate and effective controls to guarantee the records' identity and integrity. Integrity during and after transmission.
<table>
<thead>
<tr>
<th><strong>Explicitly recognise that audit trails (event histories) are part of the record</strong></th>
<th><strong>Ensure that event histories are defined as record in privacy and evidence law</strong></th>
<th><strong>Maintain control over personal data for patient autonomy through ownership of process</strong></th>
<th><strong>All access to a consumer EHR will be logged and able to be tracked back to an individual - provider, consumer or other authorised person (BA v1.9 p. 32).</strong>&lt;br&gt;<strong>All changes to the consumer’s EHR data must be versioned and retained on the audit trail in such a way that previous versions of EHR information can be accessed. (BA v1.9 pp. 141-142.)</strong></th>
<th><strong>Recordkeeping</strong>&lt;br&gt;Audit trails are part of “tracking” which is “creating, capturing and maintaining information about the movement and use of records”. International Standards Organisation, <em>International Standard: Information and Documentation - Records Management ISO 15489-1-2001 Part 1</em>, p 3.&lt;br&gt;Pittsburgh (6) Identifiable: Records must be bounded by linkage to a transaction which used all the data in the record</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Define audit trails and logs as records&lt;br&gt;• Monitor and make available to the patient access logs of records used</td>
<td><strong>Principle</strong>&lt;br&gt;Privacy principle of individual control over collection, use and disclosure of personal information including health</td>
<td><strong>Principle</strong>&lt;br&gt;Ethical principles include control over use and disclosure of personal information including health</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legislation**<br>Electronic Transactions Acts<br>Evidence Acts<br>Archival legislation

<table>
<thead>
<tr>
<th>Principle</th>
<th>Right of redress</th>
<th>Principle of patient autonomy via access and control over one’s own health information</th>
<th>C-130 The information to be retained on the consumer’s EHR access log and available for review by the consumer includes: (a) those persons that have accessed their EHR; (b) the provider organisation from which the access originated; (c) the date and time of access; (d) the nature of the access (update, view etc); and (e) the part(s) of the EHR that were accessed. See also Process J5 - Maintain access log</th>
</tr>
</thead>
<tbody>
<tr>
<td>All record actions must be tracked.</td>
<td>by both primary and secondary users</td>
<td>EHR access log and audit trail are progressively updated with each transaction</td>
<td>ISO 15489.1 10: Monitoring and auditing: compliance monitoring should be regularly undertaken to ensure that records systems procedures and processes are being implemented according to the organisational policies and requirements and meet the anticipated outcomes</td>
</tr>
<tr>
<td>ISO 15489.1: 8.3.2 Documenting records transactions: Records systems should contain complete and accurate representations of all transactions that occur in relation to a particular record...Alternatively they may be documented as audit trails which should be kept at least as long as the document to which they relate is retained</td>
<td>ISO 23081 9.5 Role of Systems: One method of recording changes is through the use of audit trails. However, while audit trails for records and business systems are essential for business continuity purposes, they may not fully meet the records management requirements to provide a complete transaction</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ISO 15489.2 Use and Tracking: The tracking of records usage within records systems is a security measure for organisations. It ensures that only those users with appropriate permissions are performing records tasks for which they have been authorised. The degree of control of access and recording of use depends on the nature of the business and the records they generate.

**Law and ethics**
Rights to privacy in terms of a consumer gaining access to who saw what and when require tracking.

Statutory and common law rights of privacy.

<table>
<thead>
<tr>
<th>Ensure patient and provider identifiers accurately identify individuals</th>
<th>Ensure statutory penalties are appropriate for the misuse of identifiers</th>
<th>Minimise potential harm caused by misuse of identifiers</th>
<th>Each consumer and their EHR information will be uniquely identified within HealthConnect by use of a single unique identifier able to be linked to any future National Health Identifier. (BA v1.9, p. 30)</th>
<th>Recordkeeping</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Verify the identity of the consumer (patient) and</td>
<td>Principle</td>
<td>Principle</td>
<td>Processes from registration</td>
<td>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</td>
</tr>
</tbody>
</table>
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 person.

**Autonomy.**
Record linkages undermine patient autonomy if the patient has not consented to the linkage

<table>
<thead>
<tr>
<th>Principle</th>
<th>Agency perspective:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C-164 HealthConnect solutions should be prepared to adopt the national health identifier as the authoritative source of unique consumer identification for HealthConnect, when the identifier becomes available.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>C-168 When and if it becomes available, a national health provider identifier should be adopted by HealthConnect solutions as the authoritative source of unique provider identification for HealthConnect.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>C-81 HealthConnect solutions (and particularly the HealthConnect consumer registration service and consumer registration system) must include functions that allow the consumer to identify themselves online, by post or by telephone (to a consumer registration agency or to the consumer registration service) and to: (a) Change a</strong></td>
<td></td>
</tr>
</tbody>
</table>

| **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; Health Records Acts. eg 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.

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.
<table>
<thead>
<tr>
<th>Document policies, rules and procedures as recordkeeping metadata</th>
<th>Ensure appropriate rules are linked to the record transaction</th>
<th>Ensure appropriate rules are linked to the record transaction</th>
<th>Processes that define responsibilities: A. Administering Health Connect Process A1- Establish HealthConnect operational policies and standards (Expanded as C-69) B9-C-75 Coordinate HealthConnect records management functions Provider records management responsibilities. (BA v1.9 p. 77.)</th>
<th>Recordkeeping ISO 15489 provides guidance on determining the responsibilities of organisation for records and records policies, procedures, systems and processes ISO 15489.1 Policy and Responsibility 6.1: An organisation seeking to conform to this part of ISO 15489 should establish, document, maintain and promulgate polices,</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Document policies and procedures as recordkeeping controls (see also reliability).</td>
<td>• Ensure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Principle</td>
<td>Principle</td>
<td></td>
<td>Recordkeeping ISO 15489 provides guidance on determining the responsibilities of organisation for records and records policies, procedures, systems and processes ISO 15489.1 Policy and Responsibility 6.1: An organisation seeking to conform to this part of ISO 15489 should establish, document, maintain and promulgate polices,</td>
</tr>
<tr>
<td></td>
<td>Principles of evidence and admissibility that demonstrate the rules that governed a record are linked to that record.</td>
<td>Duty to act according to rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle</td>
<td>Persistent link of rules with individual transactions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Document changes to policies through time.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policies and procedures as metadata are essential to record authenticity.</td>
<td>Legal duty to record actions required by policies, rules and procedures.</td>
<td>Legal duty to record actions required by policies, rules and procedures.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ISO 23081, 10.3.1 Metadata about the business rules, policies and mandates at point of records capture: ...metadata should document records compliance with business rules and policies, regulatory and other requirements for creating and managing records...a) identify the specific metadata scheme or schema used in organisational business systems b) capture the business rules or other system controls that regulate record creation and management c) capture the business rules or other system controls that regulate metadata creation and management...e) capture the business rules or other system controls that regulate access and rights to records f) document the mandate or other regulatory requirement for record creation and/or management

*Depending on jurisdiction*
| Define and capture responsibilities of each participant at each level of aggregation in the architecture | Ensure participants are legally accountable through records systems that capture their identity and competencies in relation to each and every role | Ensure participants are morally accountable through records systems that capture their identity and competencies in relation to each and every role | The original and updated versions of the event summary will contain the identity of the provider submitting the event summary (BA v1.9 p. 55) Linkage to ‘professional registration’ as a criterion for HealthConnect registration. |}

- expansion of ISO 15489 section 8.4 and ISO 15489.2 Section 3.2 (Design and Implementation of a records system) then also specific DIRKS methodology.

- Pittsburgh (2) Responsible: Recordkeeping systems must have accurately documented policies, assigned responsibilities, and formal methodologies for their management.

- IP1 Benchmark A.1 Expression of Record Attributes and Linkages to Records

**Legislation**
Evidence Acts: admissibility provisions

**Ethics**
Duty to act according to rules (deontology).
| Capture and maintain agent recordkeeping metadata (Record agents: senders, recipients of communication) | **Principle** | Ascertain legal rights, obligations and powers of consumers, providers, and organisations delivering components of HealthConnect, and of the HealthConnect governing body itself. Rights of intellectual property (economic and moral) and access rights of owners, authors and users at each level of record aggregation. Different roles of organisation and individual provider, although the same person may have more than one juridical role. | **every role** | This will require their professional registration body to have been previously recognised and registered with HealthConnect (BA v1.9 p. 31). National health provider directory ... If approved, with appropriate regulatory backing ... (BA v1.9 p. 124) Process M5 - Provide a national Health Provider Directory service. C-94 Registration of an individual provider | Records systems need to capture these changes. This contextual information is necessary for understanding records. ISO 23081 10.2.1 Metadata about records at point of record capture: ...metadata about the record should b) identify and describe the persons involved in records creation ISO 15489.1 6.3 Responsibilities: Records management responsibilities and authorities should be defined and assigned, and promulgated throughout the organisation so that, where a specific need to create and capture records is identified, it should be clear who is responsible for taking the necessary action. IP1Principle Ensure record attributes are inextricably linked to the record. ISO 23081 9.3.2 Creating and Maintaining metadata: Metadata about creating or altering metadata about a record should also be defined and maintained |
| --- | **Principle** | Moral principle of accountability for action in a specific time and place. Ethical motives for action | | | | |
| Creating and Updating Rules | HealthConnect. (BA v1.9 p. 106.)  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Event summaries submitted by a provider need to be attributable to that provider over time.</td>
<td>C-79 HealthConnect solutions must support the process of registering a consumer … (b) Capture consumer’s registration details and C-80.</td>
</tr>
<tr>
<td>Manage registers and identity information as part of a record transaction.</td>
<td>ISO 23081 9.3.9.2 Authenticity and fixity of metadata: Records management metadata need to be maintained as they are and, in case change is needed, rules should be in place to govern the process. These should include rules to document reasons for the changes, the changes themselves and the authorised agents involved. Metadata providing detail about the creation of or change to the metadata record itself should be maintained. This should include information about any agents associated with the creation or change and the type of activity that was undertaken, for example: created, modified, checked, deleted. In addition the version of the metadata schema used to define and populate the metadata elements should be identified.</td>
</tr>
</tbody>
</table>
| Adopt appropriate authentication (see also access privileges) | Legislation  
Health Practice Acts (states)  
Health Records Acts (states)  
Copyright Act: moral rights provisions |
| Check registration and identification details with external sources (each one needs a transmission record, receipt of details, incorporation) | Ethics  
Deontology: Ethical obligations from identified rights. |
<table>
<thead>
<tr>
<th>Principle</th>
<th>Ensure records created under contract include full recordkeeping arrangements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principle</strong></td>
<td>Provenance and record agency</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>Record accountability</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>Contractual liability must be the subject of an express or implied guarantee of truth (or falsity). Other elements are fair conduct, unconscionable conduct and good faith in contract negotiation supported by case law.</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>Moral obligation to be truthful in contracts, that is, not to provide misleading information about what is intended in the contract.</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>It is envisaged that there will be a limited number of HRS implemented across Australia each of which may be operated by public or possibly private organisations referred to as Approved EHR Managers (AEMs) (BA v1.9 p. 42.)</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>Each AEM will be responsible for the security and access control of EHR information held in the HRS that they operate. The AEM must protect the confidentiality, integrity and availability of the EHR. (BA v1.9 p. 112)</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>Process A-A3 - C-71</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>Outsourced functions [See also system view of HRS processes]</td>
</tr>
<tr>
<td><strong>Principle</strong></td>
<td>C-79 HealthConnect solutions must support the process of registering a consumer by delivering sub-processes with</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recordkeeping</th>
<th>Virtue ethics: character and roles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recordkeeping</strong></td>
<td>National Archives of Australia, Outsourcing, Accountability and Recordkeeping, Archives Advice 12, Issued August 1997/Revised August 2002.</td>
</tr>
<tr>
<td><strong>Recordkeeping</strong></td>
<td>National Archives of Australia, Contracting out your records management, Archives Advice 14, Issued September 1997/Revised August 2002.</td>
</tr>
<tr>
<td><strong>Recordkeeping</strong></td>
<td>ISO 15489.1 Scope: This part of ISO 15489 provides guidance on determining the responsibilities of organisation for records and records policies, procedures, systems and processes</td>
</tr>
<tr>
<td><strong>Recordkeeping</strong></td>
<td>ISO 15489.1 Policy and Responsibility 6.1: An organisation seeking to conform to this part of ISO 15489 should establish, document, maintain and promulgate polices.</td>
</tr>
</tbody>
</table>

Livia Iacovino: Recordkeeping, Legal and Ethical Principles and Requirements for HealthConnect: Template V1.0
July 2005
<table>
<thead>
<tr>
<th>Implement retention periods for all classes of records at all levels of the HealthConnect architecture</th>
<th>Determine both statutory requirements and potential litigation needs in relation to retention</th>
<th>Protect the community from harm and provide for accountable actions in the public interest</th>
<th>Implement the following functionality: … procedures and practices for records management to ensure that its business need for evidence, accountability and information about its activities is met. ISO 15489.1: 8.3.4 Distributed management: Records systems should be capable of supporting alternative options for the location of records. <strong>Law</strong> Office of the Federal Privacy Commissioner, <em>Information Sheet 14-2001: Privacy Obligations for Commonwealth Contracts</em>, <a href="http://www.privacy.gov.au/publications/IS14_01_print.html">http://www.privacy.gov.au/publications/IS14_01_print.html</a> <strong>Ethics</strong> Deontology: duty to tell the truth. <strong>Recordkeeping</strong> ISO 15489.1. 9.2 Determining how long to retain records: Decisions about how long records should be maintained within a records system are based on an assessment of the regulatory environment, business and accountability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement retention periods for all classes of records at all levels of the HealthConnect architecture</td>
<td>Determine both statutory requirements and potential litigation needs in relation to retention</td>
<td>Protect the community from harm and provide for accountable actions in the public interest</td>
<td>Implement the following functionality: … procedures and practices for records management to ensure that its business need for evidence, accountability and information about its activities is met. ISO 15489.1: 8.3.4 Distributed management: Records systems should be capable of supporting alternative options for the location of records. <strong>Law</strong> Office of the Federal Privacy Commissioner, <em>Information Sheet 14-2001: Privacy Obligations for Commonwealth Contracts</em>, <a href="http://www.privacy.gov.au/publications/IS14_01_print.html">http://www.privacy.gov.au/publications/IS14_01_print.html</a> <strong>Ethics</strong> Deontology: duty to tell the truth. <strong>Recordkeeping</strong> ISO 15489.1. 9.2 Determining how long to retain records: Decisions about how long records should be maintained within a records system are based on an assessment of the regulatory environment, business and accountability.</td>
</tr>
</tbody>
</table>

Implement retention periods for all classes of records at all levels of the HealthConnect architecture

- Appraise and retain/dispose

Determine both statutory requirements and potential litigation needs in relation to retention

- Apply other legal requirements re:

Protect the community from harm and provide for accountable actions in the public interest

*HealthConnect will be a repository service for consumers’ lifetime health records. BA v1.9 p. 37 and EHR data will be permanently recorded and preserved subject to legal constraints. (BA v1.9 p. 34.)*
| Principle | Duty to preserve records before litigation commences. Deletion principle in privacy laws may, in some circumstances, conflict with recordkeeping principles of reliability and authenticity. Even if destruction is legal it may deny potential litigants access to evidence needed to support their case. Duty to prevent harm in public interest. |
| Principle | Ethical duty to preserve records before litigation commences and for accountable actions. Information once submitted to HealthConnect may not be deleted or altered; however corrections or amended information may be included in the EHR by issuing revised versions of the information which will be used in place of the earlier versions with appropriate annotations. (BA v1.9 p. 33) Should factual information on the record be considered incorrect, the consumer will be able to request, via the HCCAS that it be changed. The rules determining whether a correction is made will be set out by the HealthConnect governing body....A consumer will also be able to request that a comment be added to an event summary ... may request that a particular event summary be withdrawn from view....In all cases the original information will be kept for medico-legal and audit purposes, but will no longer be disclosed by HealthConnect. (BA v1.9 p. 55) If a consumer deregisters from HealthConnect, the information in their HealthConnect record will be withdrawn from view but |

See also access by third parties and secondary use

Integrity

Principle

Duty to preserve records before litigation commences.

Deletion principle in privacy laws may, in some circumstances, conflict with recordkeeping principles of reliability and authenticity.

Even if destruction is legal it may deny potential litigants access to evidence needed to support their case.

Duty to prevent harm in public interest.

Information once submitted to HealthConnect may not be deleted or altered; however corrections or amended information may be included in the EHR by issuing revised versions of the information which will be used in place of the earlier versions with appropriate annotations. (BA v1.9 p. 33)

Should factual information on the record be considered incorrect, the consumer will be able to request, via the HCCAS that it be changed. The rules determining whether a correction is made will be set out by the HealthConnect governing body....A consumer will also be able to request that a comment be added to an event summary ... may request that a particular event summary be withdrawn from view....In all cases the original information will be kept for medico-legal and audit purposes, but will no longer be disclosed by HealthConnect. (BA v1.9 p. 55)

If a consumer deregisters from HealthConnect, the information in their HealthConnect record will be withdrawn from view but

requirements and the risk. Initially, such decisions should involve the unit administering the specific business activity, the designated records manager and others as required, in compliance with the external and internal records management policies or standards and the requirements for records associated with the specific business activity. Statutory or other regulatory requirements may demand minimum retention periods or submission to an authorizing body such as an archival authority or auditors for any necessary approval. The rights and interests of all stakeholders should be considered when determining how long records need to be maintained. The decisions should not be made intentionally to circumvent any rights of access.

Records retention should be managed to....a) meet current and future business needs by ....3) eliminating, as early as possible, and in an authorised systematic manner, records which are no longer required...c) meet the current and future needs of internal and
| Implement access privileges for all participants | Ensure doctors and other health care providers abstain from disclosing information imparted to them in the course of a professional | Ensure doctors and other health care providers abstain from disclosing information imparted to them in the course of a professional | Consumers will have control over who may access their HealthConnect EHR. (BA v1.9 p. 31.) Consumers will have access to HealthConnect to view and, in | external stakeholders... |

**Legislation**  
Note: issue of jurisdiction that applies has first to be determined.  

Archives Acts Evidence and Discovery  
*Health Records Act 2001 (Vic)*, HPP 4.2 provides that a health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless permitted by law, or not contrary to a law. Information can be deleted related to a child once the individual attains twenty five years, or in any case seven years after the last occasion on which a health service was provided to the individual.  

**Ethics**  
Utilitarianism

Livia Iacovino: Recordkeeping, Legal and Ethical Principles and Requirements for HealthConnect: Template V1.0  
July 2005
<table>
<thead>
<tr>
<th>Principle</th>
<th>Professional relationship unless authorised by the patient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical and legal duty of confidentiality not to disclose information imparted in the course of a professional relationship</td>
<td></td>
</tr>
<tr>
<td>Ethical duty of confidentiality of secrets</td>
<td></td>
</tr>
<tr>
<td>Professional ethical duty of healthcare providers to protect the contents of communications imparted to them in the course of a professional relationship</td>
<td></td>
</tr>
<tr>
<td>Duties of users of HealthConnect?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Principle</th>
<th>the future, contribute to their EHR information and, also, to review the access log for their EHR and to set preferences that control access to the EHR. (BA v1.9 p. 31.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider access to view a consumer’s HealthConnect EHR implies that the provider requires access to the information for clinical purposes.</td>
<td></td>
</tr>
<tr>
<td>Each provider organisation will be responsible for controlling its personnel’s use of HealthConnect information and for ensuring that the individual provider (or any other person) accessing the consumer’s EHR on behalf of the provider organisation does so for valid clinical reasons, and that the provider/person is identified to HealthConnect.</td>
<td></td>
</tr>
<tr>
<td>Providers once authorised will be able to access all parts of the consumer’s HealthConnect EHR.</td>
<td></td>
</tr>
<tr>
<td>All access to a consumer EHR will be logged and able to be tracked back to individual - provider, consumer or other</td>
<td></td>
</tr>
</tbody>
</table>

| AS ISO 15489-2, 4.2.5.1 A formal instrument that identifies the rights of access and the regimes of restrictions applicable to records is a necessary tool to manage records in organisations of all sizes and jurisdictions |
|-----------|---------------------------------------------------------------------------------------------------|
| AS ISO 15489-2, 4.2.5.2: Access classifications also apply to people, both those who are responsible for managing the access-classified records and others with rights of access....A records system has to manage user permissions specific to itself |
| AS ISO 23081 10.3.1 Metadata about business rules, policies and mandates at point of record capture....e) capture the business rules or other system controls that regulate access, and rights to records |
| AS ISO 23081 10.5.1 Business process metadata at point of record capture: Business process metadata at point of record capture should...d) document the security and access rules for business processes and transactions |
**Principle**
Access rights to records

**See also**
consent
third party access
audit trails/tracking identifiers

---

**Control.**

**HealthConnect participants will be obliged to abide by privacy legislation and by specific HealthConnect privacy rules.** (BA v1.9 p. 32)

Note: once the EHR is downloaded into a CIS, providers become responsible for its security and access (BA v1.9 p. 33, p. 6).

Example of related processes C-139 Unless otherwise agreed with the HealthConnect governing body, the HRS should manage access to a consumer’s EHR information as follows: (a) The HRS should establish a unique session with each user seeking access at any particular time. On receiving the first message seeking access in each session, the user’s identity and access privileges must be authenticated and confirmed against subsequent incoming messages.

---

Interpares A2: The creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation and destruction of records.

**Law**
Tort and contract law re: confidentiality. Legal requirements for healthcare providers to disclose for research, health reporting, health and insurance administration and litigation. Statutes: eg The Health Records Act 2001 (Vic); Health Information Privacy Act 2002 (NSW); Health Records (Privacy and Access) Act 1997 (ACT); and the Privacy Act 1988 (Cth): Data security (NPP 4.1) requires a health service provider to have security safeguards in place to protect health information (in electronic form, paper, audio or video tapes) against both accidental and intentional breaches of confidentiality.

National Health Privacy Code (NHPC): Draft
<table>
<thead>
<tr>
<th>Maintain records of express and informed consent of consumers to both primary AND secondary users of HealthConnect records</th>
<th>Ensure consent to participate by the patient or provider is informed</th>
<th>Ensure patient has capacity to consent</th>
<th>Consumer participation in HealthConnect will be voluntary and nondiscriminatory. (BA v1.9 p. 30)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure consent by the patient to secondary of personal data is explicit</td>
<td>Ensure agents representing patients are appropriate</td>
<td>Consumer consent for participation in HealthConnect remains valid until deregistration. (BA v1.9 p. 31.)</td>
<td></td>
</tr>
<tr>
<td>Principle</td>
<td>Allow individual control/choice as moral agents</td>
<td>Consumers will, as part of the sign up process, consent to an “emergency access override”</td>
<td></td>
</tr>
<tr>
<td>Privacy requires informed consent from participants for the collection, use and disclosure of personal information and explicit consent for the release of information to third</td>
<td>Principle</td>
<td>Recordkeeping ISO 15489.1 7.1 Records are created, received and used in the conduct of business activities. ...a) determining what records should be created in each business process, and what information needs to be included in the records.</td>
<td></td>
</tr>
<tr>
<td>Ensure controls over consent update processes.</td>
<td>Respect for patient autonomy is not compatible with standing consent.</td>
<td>Law Private healthcare providers are bound by the 10 National</td>
<td></td>
</tr>
<tr>
<td>Ensure consent control list and event summary to which it relates</td>
<td></td>
<td>HealthConnect governing body determinations on misconduct. Penalties for misuse of data.</td>
<td></td>
</tr>
</tbody>
</table>

**Ethics**
- Respect for a person’s privacy.
- Confidentiality
  - Section 1.1(1) of the Australian Medical Association’s (AMA) Code of Ethics (2004).

**Confidentiality**
- Consumer participation in HealthConnect will be voluntary and nondiscriminatory. (BA v1.9 p. 30)
- The consumer must have given informed consent before their EHR and other personal information can be collected, accessed, used or disclosed by HealthConnect. This will form part of the initial consumer consent process. (BA v1.9 p. 30.)
- Consumer consent for participation in HealthConnect remains valid until deregistration. (BA v1.9 p. 31.)
- Consumers will, as part of the sign up process, consent to an “emergency access override”
is persistently linked.

- Document as a record consent rules and any changes.
- Records must have an explicit and persistent link to the consent rule operating at that time the record was created.
- Expand consent list to providers and other authorised staff in organisations.

### Principle
Record authenticity

### See also
- retention
- Third party access
- Access privileges
- Consent to join
- Consent settings

### Privacy Principles (NPPs) of Privacy Act 1988 (Cth) which require consent for collection and use of health information; secure data storage; impose limitations on transborder data flows. As a general rule, under NPP 2(b), the patient must consent to the use of health information provided by her or him. However, under NPP 10.3(a)(iii) and NPP 10.3(d)(ii), no consent is required for the collection of health information if it is necessary for “the management, funding or monitoring of a health service” and “the information is in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.”

### Ethics
No arbitrary interference with privacy and protection from such interferences in law. Article 17 of The International Covenant on Civil and Political Rights 1966

### Bioethics:
Patient autonomy is...
### Manage access by third parties which conforms with relevant laws and ethics codes

- Establish appropriate rules
- Consider technological means of protecting privacy that maintain record integrity
- Monitor access via audit trails/logs of access
- Use

<table>
<thead>
<tr>
<th>Adhere to the duty of confidentiality re identified and de-identified data</th>
<th>Adhere to the moral duty of confidentiality re identified and de-identified data</th>
<th>HealthConnect will support secondary use of HealthConnect EHR information for improvement of health service delivery and research purposes, in line with strict privacy and ethical protocols, appropriate legislative requirements and monitoring of such use. (BA v1.9 p. 29.)</th>
<th>Recordkeeping AS ISO 15489, 9.7: Organisations should have formal guidelines regulating who is permitted access to records and in what circumstances. AS ISO 15489-2, 4.2.5.1 A formal instrument that identifies the rights of access and the regimes of restrictions applicable to records is a necessary tool to manage records in organisations of all sizes and jurisdictions. Pittsburgh (13), “Redactable”. Redacted version is a separate record but must be linked back to original. Pittsburgh: 9a1 Record as “Inviolate”.</th>
</tr>
</thead>
</table>
| Seek an interpretation of de-identified data and ‘potentially identifiable data’ in privacy laws. | Principle
The privacy “Purpose Limitation Principle”
Non-release of third party of information provided in one context for another unless explicit consent given. Westin’s zones limit patient data to those | Principle
Respect for a person’s moral right to privacy
Patients should retain maximum control of the uses and disclosures of their identifiable personal information. | |
<table>
<thead>
<tr>
<th>Principle</th>
<th>Contractual agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Lapse of time” archival principle</td>
<td></td>
</tr>
<tr>
<td>Authentication to ensure access is for authorised users</td>
<td></td>
</tr>
<tr>
<td>• Invoke sunset clauses in relation to access to health information (once it has been appraised)</td>
<td></td>
</tr>
<tr>
<td>• Apply “lapse of time” archival principle and notion of trusted third party</td>
<td></td>
</tr>
<tr>
<td>Secondary uses must take account of any harm to the subjects whether identified or de-identified.</td>
<td></td>
</tr>
<tr>
<td>Potential harm to an individual if information is accessed by someone who poses a threat to that person (eg domestic violence).</td>
<td></td>
</tr>
<tr>
<td>Patients should be informed that their de-identified data may be used for research or other purposes.</td>
<td></td>
</tr>
<tr>
<td>Access by third parties outside of the primary zone</td>
<td></td>
</tr>
<tr>
<td>Team, for purposes associated with management and control of HealthConnect itself.</td>
<td></td>
</tr>
<tr>
<td>All secondary uses of HealthConnect must be subject to stringent approval including review and acceptance by an ethics committee and measures that protect the privacy of individuals and the confidentiality of their personal data. The HealthConnect governing body sets and enforces the policies and guidelines for secondary uses. (BA v1.9 pp.107-108.)</td>
<td></td>
</tr>
<tr>
<td>Process B-B5. Handle applications for secondary use of HealthConnect data. This involves the establishment of relevant processes to operate under the HealthConnect rules.</td>
<td></td>
</tr>
</tbody>
</table>

### Law

No sunset clause on the disclosure of medical information about a deceased person in common law. Professors and confidentiality are enforceable in equity through an action for breach of confidence; at common law, through the action for intentional infliction of psychiatric injury and in negligence; as well as through professional codes of ethics.  

Archival/records legislation. For example in the case of personal health information in a state archive, the State Records Act 2000 (WA) s 49(2) sets a hundred year limit to protecting personal medical information from disclosure via a special provision for lapse of time for access to a medical record that is a ‘State archive’ which is at

---

3 A. F Westin (1976) Computers, Health Records and Citizen Rights, New York/Princeton, PBI, p. 10. Personal medical data is divided into three zones by Westin: (1) Primary Care (2) Supporting Activities and (3) Social and Other Uses of Health Records Data.  

---

Livia Iacovino: Recordkeeping, Legal and Ethical Principles and Requirements for HealthConnect: Template V1.0
July 2005
| Right of access to records | (healthcare providers treating the patient) should be strictly controlled. See Westin’s zones. | research purposes will be assessed through a rigorous approval process, including ethics committee assessment. Such approved purposes will only be permitted according to strict criteria, and with agreements in place to govern the handling and security of stored data within an organisation and subsequent publication of the research findings to protect individual and community privacy. (BA v1.9 p. 97)

As a part of the approval, HealthConnect will have the right to scrutinise research prior to it being published to ensure compliance with the ethics approval guidelines (BA v1.9 p. 98.)

HealthConnect’s governance structures, yet to be finalised, will contain arrangements for the independent and transparent monitoring of the role of HealthConnect in authorising and managing access to information for secondary uses. (BA v1.9 p. 96)

Assistance from Australian neighbours is available for privacy issues. (BA v1.9 p. 98.)

| See also Consent Retention | least one hundred years old. An alternative is to cover living persons only. (See also the NHPPS ‘Further Issues for Discussion’ ‘Deceased Persons’).

The “Purpose Limitation Principle” that personal information should only be collected, used or disclosed for its primary or original purpose and its use and disclosure for secondary or other purposes is subject to strict limitations. See Articles 6 (1) (b) and 7 of the European Directive of Privacy 95/45/EC. See also International Instruments on privacy.

Section 95A of the Privacy Act 1988 (Cth) provides a framework for human research ethics committees to assess proposals to access health information (including without the consent of the subject) for research, the compilation or analysis of statistics, or health service management, to weigh the public interest in those activities against the public interest in the protection of privacy. |
C4.13.3 NDS Functional Requirements. Within the HealthConnect, processing functions associated with the maintenance of the National Data Store (NDS) are required to support the production of EHR Reports (for national reporting including secondary research and planning uses). following business processes: (a) Process K3 - Maintain audit trail and National Data Store (based on inputs from HRS); and (b) Process J4 - Produce EHR Report

(BA 1.9 Specifications. p. 77.)

Ethics

The disclosure of personal information to third parties is contrary to the basic principle that individuals should be able to determine for themselves when, how, and to what extent information about them is communicated to others.8

Archival Codes of Ethics re: privacy: International Council on Archives Code of Ethics

Health Ethics Committee established under NHMRC Act 1992 (BA v1.9 p. 96)

Process K3 - Maintain audit trail and [provide information for inclusion in] the National Data Store.
Process K4 - Produce EHR Report (for national reporting including secondary research and planning uses).
COMMENTARY ON THE TEMPLATE

RECORDKEEPING REQUIREMENTS

Define record as process and capture all processes as records

The boundary of the Electronic Health Record (EHR) both as an information object and its related processes is notional in the HealthConnect models. Storing EHR event summaries will be logical rather than physical. The event summary consists of component parts stored separately, linked through a variety of mechanisms, the key one being the unique health identifier. This architecture reinforces the importance of taking a process oriented view of recordkeeping, which identifies and manages the mechanisms of production as well as the outcomes.

All event summaries form the EHR, but the “views”, “lists” and “reports” are also records. In fact the provider does not access the full record of all the event summaries, only the requested view. Additional services that stand outside the Health Record System (HRS) also create records that relate to the EHR, eg registration records. “Owning” the process embeds the record with its creator. Therefore defining the record as process is necessary to capture all the activities that create records and their metadata. To adequately protect authenticity, integrity and reliability of the EHR, each process needs to be considered from a recordkeeping perspective.

Finding: Critical absence of recordkeeping functionality.
EHR is cumulative, exists in a number of places, contains connections to data held separately such as access control lists, and views predetermined according to defined templates, indexes, access and audit logs. Each of these separate components has different processes that dictate their incorporation into the consolidated virtual EHR.

Recognise that preservation of authentic shared electronic health records is a continuous process

The preservation of authentic shared electronic health records as a continuous process is embedded in records continuum theory and practice, the International Standard ISO 15489, Records Management, and in Interpares 1 Strategies

Livia Iacovino: Recordkeeping, Legal and Ethical Principles and Requirements for HealthConnect: Template V1.0
July 2005
Report and requirements. Preservation includes the capture, ongoing access, physical preservation including migration and dealing with redundant technologies. Despite records being kept indefinitely in HealthConnect, the retention and archiving strategies are weak compared with access processes. Archiving strategy has to include documenting system processes and include metadata management.

All electronic records are technically “copies” of the “original” record. The “original” electronic record will always be a reproduction immediately after the creation of the first complete and effective record. Each time the record is accessed or forwarded, the computer creates a copy. These copies serve as originals if the essential recordkeeping metadata can be reproduced. For example, the electronic copy that is identical to the original and thus constitutes its equivalent is described in the Evidence Act 1995 (Cth) s 47(2) as “a document that is not an exact copy of the document in question but that is identical to the document in question in all relevant respects.” The Evidence Act further states that for the purpose of proof of content, a party may adduce evidence of the contents of a document in question by tendering the original document, or a copy produced by a device that reproduces the contents of documents such as a computer printout, photocopies etc. Hence, providing they retain the attributes of a record, copies that have been scanned are as good as the original. The legal acceptance of a copy that is identical in all respects translates into the electronic context where the original will always be a reproduction.

Finding: Insufficient attention to long term preservation

Comply with laws of the relevant jurisdiction

The regulatory environment can be established from positive law and its authoritative sources: statute (legislation) and case law (common law); professional, personal and corporate ethics; and industry codes of conduct and

---


9 Evidence Act 1995 (Cth) s 48(1).

10 “In common language, copy and reproduction are synonyms. For the purposes of this research, the term reproduction is used to refer to the process of generating a copy, while the term copy is used to refer to the result of such a process, that is, to any entity which resembles and is generated from the records of the creator.” InterPARES Project, Authenticity Task Force, Final Report, 28 October 2001, Appendix, footnote 10. http://www.interpares.org/documents/atf_draft_final_report.pdf. Consulted July 2005.
practice.\textsuperscript{11} It is assumed that the HealthConnect records, at least those in the National Data Store, are Commonwealth records and therefore subject to Commonwealth laws, and that there is an implicit archival control at the Commonwealth level. However, given the proposed incremental implementation by state, the involvement of the private sector, the application of state law in relation to privacy infringements, records in different parts of the architecture may be subject to different regimes. An issue to address is whether the different jurisdictions with potentially different rules may determine “ownership” based on “location” of the service/data store. There are currently limits in the federal power over the practice of medicine: \textit{Constitution Act 1900}\textsuperscript{Cth), s 51(xxiiiA): “the provision of maternity allowances, widows’ pensions, child endowment, unemployment, pharmaceutical, sickness and hospital benefits, medical and dental services (but not so as to authorise any form of civil conscription), benefits to students and family allowances.”

HealthConnect needs to address which digital preservation strategies to adopt, what and who will preserve the records and for how long, which depends on the assignment of a responsible jurisdiction at each layer of the HealthConnect model.

**Finding** HealthConnect's lack of a finalised governance structure impacted on all aspects of the project, but was particularly significant in relation to regulatory compliance, ownership and record retention.

**Capture reliable and accurate records at each level of the architecture**

HealthConnect consists of a National Coordination layer, a Health Record System layer (HRS) and a User layer (both individual clinical information systems operated by independent providers and the individual consumer level). All records at each layer of the HealthConnect architecture must be reliable. Requirements for repositories being part of the larger network are explicit in this version of the business architecture. Storage management has to be central for consistency reasons. Reliability is threatened if event histories are held by decentralised repositories.

HealthConnect has been specifically designed as a voluntary “opt-in” system for both the patient and the practitioner. Opting in and out affects the completeness of the records, and given the aim of using HealthConnect for planning purposes,

it is likely that it will not remain voluntary; the marketing features and added services for “non-participating” providers are examples. Non-reporting of events limits use of record for both primary care and for research. Setting up of the registration record requires allocating a person to an HRS. It is not clear whether this is a forever placement or whether this can change over time; but this could affect the integrity of the record over time (BA v1.9 p115).

As participants of HealthConnect, provider responsibilities include a commitment to provide accurate information to HealthConnect (BA v1.9 p. 77), recognition of consumer rights as participants in HealthConnect; participation in line with HealthConnect confidentiality and privacy agreements; and local procedures which comply with appropriate national standards to meet HealthConnect privacy and security requirements. These will include processes to control access to, and audit the use of, the provider organisations’ information system; using clinical information systems to access HealthConnect that comply with the technical requirements of HealthConnect, and maintaining security of any EHR information integrated into their clinical information systems (BA v1.9 p77).

“The provider will, on request, not send the event summary, or delete the information prior to sending the event summary” (BA v1.9 p 31) which raises issues of the mandatory elements in specific event summaries. Data quality at the time of entry is the responsibility of the provider. The consumer has the right to suppress the submission of any event summary at the time of generation (in which case it should not be submitted by the provider) and may also apply to have it suppressed after it has been added to the EHR. Consumer can request that incorrect information be corrected via an updated summary. The original version is kept.

Event summaries submitted by that provider need to be maintained and to be attributable to that provider over time. Individual providers, HealthConnect identifiers, registration details and records of deregistration need to be permanently retained by the HealthConnect provider registration service.

“There is a concern that not having access to all the facts may impede a provider’s ability to give appropriate care” (BA v1.9 p54). “Providers viewing the HealthConnect EHR will need to take into consideration that, as with manual records, the records cannot be considered 100% complete.... Indeed until HealthConnect is widely used there will be gaps in the record relating to providers who have not yet registered with HealthConnect” (BA v1.9 p55).

Future implementations of HealthConnect are expected to include consumer contributions to their records, following resolution of medico-legal and workflow concerns (BA v1.9 p4) nevertheless, stage 1 is required to be designed with
capability for consumers to supply consumer event summaries for inclusion in their HealthConnect EHR (BA v1.9 p134). Controls over this process are required for record reliability … “there are potential medico-legal issues with consumers contributing to their health records, not least because of the expectation by consumers that their contributions will be reviewed, and acted upon by providers where necessary” (BA v1.9 p65). Consumer annotations to EHR require records which are envisaged through a separate event summary form.

**Finding** The implications on record reliability of patients who contribute to and amend their record have not been adequately considered. Full participation in HealthConnect and patient’s right to ask the provider not to include an event means that the most reliable record will be the provider’s local records.

**Capture authentic records at all levels of the HealthConnect architecture**

HealthConnect is a national network of EHR repositories with each consumer’s EHR being stored in a single HRS. A copy of the EHR material is to be transmitted to the National Data Store (NDS) for archiving and long-term retention (Bv1.9, pp 41-42). The NDS is managed by (or on behalf of) the HealthConnect governing body and aggregates EHR information sent from all HealthConnect EHR datasets to support: (a) Reporting across the national HealthConnect population for use in research, planning and management of the HealthConnect program; (b) Review, development and management of HealthConnect metadata; and (c) Maintenance of archival copies of each EHR to support recovery of records (if corrupted at an HRS), allow access for secondary use without impacting operational performance, and support ad-hoc access for specific enquiries (BA 2004, p. 113).

Each HRS is a system that provides EHR storage services. The primary functions of the HRS are to store event summaries that are contributed to the EHR by participating consumers and providers; to maintain the confidentiality, integrity, availability and non-repudiation of an individual consumer’s EHR; to present views of the EHR in response to requests by participating consumers and providers, subject to the consumer’s consent and the privacy, security and access control policies established by HealthConnect. It is envisaged that there will be a limited number of HRS implemented across Australia each of which may be operated by public or possibly private organisations referred to as “Approved EHR Managers” (AEMs) (BAv1.9, pp 41-42). Systems sitting outside of HealthConnect are a major authenticity issue in terms of consistency between repositories.
Record integrity during and after transmission of each request (time stamps, error logs) will also depend on how the source system interfaces with HealthConnect. Transmission and authentication data include metadata that needs to be persistently linked with the record.

- all changes to EHR records must maintain records
- all uses of EHR records, including reporting across EHR create records

Each access, view or list is a recordkeeping transaction and therefore a record. As the summary data will change over time, the system has to ensure that a previous view is the same as the “original” one. Recreating the view is a major authenticity question. Will every piece of data be time stamped? Or will the result of views be preserved? See C-152 event summaries linked to defined views and lists by metadata (BAv1.9 Specifications, p. 73).

**Finding:** Not all HealthConnect business processes will create a record and be retained for an appropriate period from the perspective of the functions of HealthConnect’s central authority, the Health records systems and the clinical system.

Record integrity is most at risk during transmission of data. Patient information could be penetrated at the HRS level or while a HRS transmits an EHR to another HRS or to the NDS or the NDS when it transmits reports, all of which is left largely to the private sector. Previous technical requirements for HealthConnect included provision for health virtual private networks (VPNs) to provide a secure encrypted private network overlay over the Internet. BA v1.9 includes VPNs as an option in the system. HealthConnect will use Public Key Infrastructure (PKI) for providers, while patients will access their record via a web portal using identification and authentication via a PIN/password aligned with their Medicare smartcard (BAv1.9 Specification, p. 53).

**Finding:** Whether these security measures prove to be sufficient protection from ever increasing cyber attacks they must be assessed in terms of the trustworthiness of all participants and the technologies and procedures available at any given point in time.

**Authentication and authenticity**

In common usage, authentication is understood as a declaration of a record’s authenticity at a specific point in time by a juridical person entrusted with the authority to make such declaration… Digital signature and public key infrastructure (PKI) are examples of technologies that have
been developed and implemented as a means of authentication for electronic records that are transmitted across space. Although recordkeepers and information technology personnel place their trust in authentication technologies to ensure the authenticity of records, these technologies were never intended to be, and are not currently viable as a means of ensuring the authenticity of electronic records over time.12

Digital signatures are a “seal” that ensures the continuing integrity of records held in electronic systems. The application of a digital signature permits detection of any alterations to the record, and thus provides a means to verify an authentic record.13 The unique identifier of the relevant digital certificate and its issuing authority; details of the digital signature attached to the record; and date and time stamps showing when a digital signature was successfully applied or validated are recognised in Recordkeeping Metadata Standard for Commonwealth Agencies.

Finding: There was no differentiation made between authentication and authenticity in HealthConnect.

Explicitly recognise that audit trails (event histories) are part of the record

“Tracking” is defined in the ISO records management standard as “creating, capturing and maintaining information about the movement and use of records.”14 Tracking provides an auditable trail of record transactions, ensuring that event histories are part of the record. Event histories or audit trails of a record’s amendment, management and use are essential for privacy protection, in particular in relation to checking on privacy infringements as opposed to preemptive approaches such as authentication.

It is important for privacy rights in terms of a patient gaining access to who saw what, when and whether their privacy has been infringed. This is another example of a conflict between identifiers increasing privacy risks and at the same time providing controls on who has used the data for the data subject’s control,

Transactional data collected, eg how often a patient or doctor accesses the system must be included in the meaning of personal privacy.

HealthConnect provides access to event histories for checking unauthorised access by primary users only. For example, all access requests and results require a record of transaction. Process G3-Retrieve/use EHR Information (BA v1.9 Specification, p 59). This is about consumers being able to monitor who sees their EHR. There is a requirement for HealthConnect to provide consumers with access to an audit trail detailing who has accessed which parts of their HealthConnect health information, necessitating both individual providers and provider organisations to be uniquely identifiable... these clinical support staff...will not be individually registered on HealthConnect but will need to be identified to HealthConnect by the organisations to fulfill monitoring and audit requirements in a manner acceptable to consumers. Procedures to support this requirement are being developed (BA v1.9 p74).

The audit trail will display the name of the organisation, the user who has accessed the information and the various parts of the participants’ health records that were accessed (BA v1.9 p74; see also Audit trails of logs as messages F1-C-120, Specification, p. 55). Access logs detail individual access to EHR records (including emergency override access) by providers, consumers, HealthConnect registration agencies and HealthConnect system administration functions.

The EHR access log is to be available to the consumer for review at any time and is to be automatically updated by the HRS application whenever the EHR is accessed. Information to be recorded on the EHR access log and audit trail includes:
(a) a unique sequence number for all transactions (including accesses);
(b) the date and time of transaction/access;
(c) a unique identifier for the person (and the identity of any individual provider) and, where relevant, the provider organisation from which the access was performed;
(d) for EHR inputs: (1) identification of the type of information inserted into the EHR including the type and version of any event summary; (2) the complete event summary transaction (including header information) for each and every event summary received by the HRS; and (3) the event summary status indicator for each event summary, indicating whether the event summary is a new event summary or a replacement event summary; and
(e) for EHR outputs (including notifications): (1) identification of the type of information retrieved from the EHR including the type and version of any query, view or trigger event and any query parameters; and (2) the complete output transaction (for example, the view, the list, the
HealthConnect notification or the individual event summary)…; (BA v1.9 pp141-142).

While access logs are covered, recordkeeping logs are not. An access log is to be maintained of all access to the National Data Store but this does not appear to be available to patients (BA v1.9 p157). The requirements are for access to the HRS, rather than the NDS, so there is an issue about whether the consumer will ever know how their health data is used for secondary/reporting purposes.

Recordkeeping requirements include:

- Ensure reports are re-created as records (as for views) for accountability purposes
- Preserve report and linkage parameters
- Ensure that renditions are preserved and accessible overtime.
- Keep records of applications, including ethics clearance both internally within HealthConnect and external organisations, consideration, decisions, processes (algorithms being applied), results, monitoring conditions of agreement/publication.
- Adopt a layer approach: anonymised data; encoded data; identified data.
- Preserve anonymising rules as essential metadata with the redacted version.

**Finding:** Tracking of all users will be kept but not persistently linked to the records accessed. Even though logs for all uses of HealthConnect will be logged, the system does not provide patients with access to secondary users and uses of their records. There is no articulation of the audit trail as part of the record, and therefore providing statutory rights of access.

**Ensure patient and provider identifiers accurately identify an individual**

The national health identifier will provide unique identification of a patient/client within the Australian health system. “… from the point of view of the security of personal data the presence of an identifier rather than the full personal information of an individual must be said to provide some protection for private
individuals should a subset of the records fall into the wrong hands.” It is essential that the correct person identity is attached to any health event. HealthConnect must obtain national acceptance of unique health identifiers explicitly by a social and legal mandate.

Patient authentication is rolled up in the registration and identification on first joining HealthConnect. The national consumer identification service undertakes identification via patient details which include their unique identifier either it authenticates the consumer’s identity by reference to appropriate reference database, or if not already uniquely identified, authenticates patient identity by inspection of documents and certifies that evidenced identity matches with proposed consumer registration details, allocates and records and/or activates unique HealthConnect identifier and record consumer identification information including National Health Identifier (if available). Obtains and validates consumer access control list (list of provider organisations which may access the consumer’s EHR). Consumer registration is run by the consumer registration service that may be outsourced. The consumer index and the registration record are held in a registration database; a copy goes to HRS, however the responsibility is at the national level.

See C4.5.3 Consumer Registration Requirements – Consumer Registration Service (BA v1.9, Specification, p. 31). Online process should contain the same recordkeeping for all changes to records, control list, individual details, providers’ lists, surrogate addition/discontinuation; update of Consumer Index subsystem (mechanisms/tracking of change); notification/distribution of changes to relevant HRS; consumer authentication; update and align Medicare smartcard; and audit trail. Where is notification to appropriate HRS of changes? C4.6.3 Provider Registration Requirements – Provider Registration Service (Specification BA v1.9 p. 48). Where is notification to appropriate HRS of changes?

C-79 HealthConnect solutions must support the process of registering a consumer…
(b) Capture consumer’s registration details and:
(1) if the consumer is already identified (such as by possession of a Medicare smartcard), authenticate the consumer’s identity by reference to appropriate reference database, or
(2) if not already uniquely identified, authenticate client identity by inspection of documents and certify that evidenced identity matches with proposed consumer registration details.

(c) If authenticated identity is provided, allow the consumer to be known by a familiar form and/or alias within HealthConnect.
(d) Allocate and record and/or activate unique HealthConnect identifier and record consumer identification information including National Health Identifier (if available).
(e) Obtain and validate consumer access control list (list of provider organisations which may access the consumer's EHR)...
(BA v1.9 Specification, p. 25)

C-80 HealthConnect solutions (and particularly the HealthConnect consumer registration system) must include functions that provide for:
(a) a registered consumer (or a surrogate operating in accordance with the consumer's interests and the HealthConnect rules) to amend the consumer's HealthConnect registration details, access control list and appointment of agents/surrogates.
(b) Amendments to consumer details being submitted (after authentication of identity)...
(c) The HealthConnect consumer registration service adding a National Health Identifier (when available) to the consumer's registration details.
(d) The consumer (or surrogate) updating and validating consumer access control list, with option to identify any providers to be notified of their approval to access the consumer's EHR.
(e) Consumers and consumer registration agencies having access to search functions that assist in locating provider organisations to be added to a consumer's access control list (BA v1.9 Specification, pp. 27-28).

Finding: Record metadata include patient and healthcare identifiers held centrally in national directories which map to the consumer's SEHR. Identifiers are central to the HealthConnect processes.

Document policies, rules and procedures as recordkeeping metadata

Recordkeeping and information management incorporating recordkeeping has a much higher priority as a governance issue in BA v1.9 than previously acknowledged (see recordkeeping issues on versions, agreements, rules, policies). Recordkeeping metadata includes the rules, provider and consumer directories essential to the record's reliability and authenticity. Adoption, negotiation and promulgation of standards to apply in HealthConnect (BA v1.9 Specification C-166, p. 79) require records, yet they are outside EHR transaction system.
Of specific note is C-69 (a)7 requiring rules to be established about recordkeeping “managing HealthConnect records and information including maintenance and use of audit trails, and the retention, archiving, splitting and combining of records” (BA v1.9 Specification p. 18) and “(b) define rules and promulgate standards governing the structure, content, source, destination and interchange of HealthConnect information – including EHR information, registration information, eHealth messages, audit trails, access logs and information required for systems administration and management” (BA v1.9 Specification p. 19). As administrative records, such records would be normally part of the governance agreements, however, as the HealthConnect Program office is under the Federal jurisdiction in the short term all records of development will by default be federal records.

**Finding:** Recordkeeping metadata is essential to the record’s reliability and authenticity. In HealthConnect they are outside EHR transaction system.

**Define and capture responsibilities of each participant at each level of the HealthConnect architecture**

The capture of recordkeeping agents, their roles and their competencies is necessary to determine their legal and ethical responsibilities (see also authentication based on competencies, as well as the responsibilities of those running outsourced services). While health service providers are often collectively referred to as “providers”, the business architecture identifies significantly different roles for “individual providers” and “provider organisations”. In particular, it is only a “provider organisation” which obtains the right to access a consumer’s HealthConnect EHR information. On the other hand, it is only an “individual provider” registered with HealthConnect that can have responsibility for clinical information submitted for inclusion in the consumer’s EHR. To enable providers to fully utilise HealthConnect services, sole practitioners would therefore have dual registration as both a provider organisation (for access) and as an individual provider (for submission of event summaries), (see BA v1.9 Specification p. 36). In relation to consumer registration:

A combination of organisational entities will work together in their respective roles to establish and maintain HealthConnect consumer registration. As discussed in Section 8 of the Business Architecture, the key roles for entities involved in consumer registration are:

- HealthConnect governing body;
- a HealthConnect consumer registration service with national coverage; and
• consumer registration agencies appointed by the HealthConnect governing body; with some support and assistance being provided by
• HealthConnect consumer access services.
Although these have been identified as separate roles that may potentially be performed by different organisations (particularly in the longer-term), in some implementations, one organisation may elect to carry out several of the roles simultaneously (e.g., consumer registration agency and HealthConnect consumer access service) (BA v1.9 Specification p. 23).

**Finding:** Roles and responsibilities associated with the different layers and different copies of the same data are not clearly identified and delineated.

**Ensure records created under contract include recordkeeping arrangements**

The intended use of private providers for many operational services of the HRS including registering and managing consumer and provider participation involve records management activities. Even ensuring the security of public networks is given to the contractor. A number of HealthConnect Registration Agencies may be contracted to perform front line registration functions. Approved EHR Managers will be contracted to run the HRS; HealthConnect Consumer Access Services will be contracted to support customer interaction with HealthConnect; and Provider eHealth Access Services will be contracted to support providers interacting with HealthConnect (BA v1.9 p163).

...all HCCAS [HealthConnect Consumer Access Services] operators must be licensed by the HealthConnect governing body. As part of being licensed, they must agree with reasonable conditions relating to compliance with HealthConnect policies, maintaining confidentiality and security of HealthConnect information... (BA v1.9 p117).

**Finding:** Different parts of the system all with recordkeeping requirements will be managed by different suppliers.

**Develop and implement retention periods for all classes of records at all levels of the HealthConnect architecture**

In earlier versions of the BA there was a requirement for “archiving” albeit a very broad definition. “Archiving. Establish rules and manage the archiving of event
summaries according to type, age etc while ensuring that the provision of the longitudinal health record is not compromised. Archiving legislation must be supported”.16

In BA 1.9 it is proposed that retention periods for registration records within national data set be retained indefinitely. Individual providers, their HealthConnect identifier, registration details and records of deregistration are to be permanently retained by HealthConnect provider registration service (Process C-103 (e), BA v1.9 Specification p46). Deregistration, withdrawal of consent permissions by consumer mean that the whole or parts of the record are triggered not for release - becoming an access issue rather than a true withdrawal. The records (even when consent is revoked) remain available for secondary use. The record in the HealthConnect Registration Agent is maintained separately and retained “indefinitely”. “Information, once submitted to HealthConnect may not be deleted or altered; however corrections or amended information may be included in the EHR....” (BA v1.9 p33). “The EHR data will be permanently recorded and preserved subject to legal constraints” (BA v1.9 p34) and “if a consumer deregisters from HealthConnect, the information in their HealthConnect record will be withdrawn from view, but will not be deleted” (BA v1.9 p34). For consumer who cancels his/her registration, information in their HealthConnect record will be withdrawn from view but will not be deleted. This is explained as part of the informed consent process. Any future event summaries submitted to HealthConnect will be rejected and providers will no longer be able to view the record. This information remains available for medico-legal purposes and, should the consumer wish to reinstate their HealthConnect participation at some time in the future, the block on viewing could be reversed. Information in a “withdrawn from view” record will also continue to be available for secondary reporting uses (BA1.9 p 61). Temporary suspension pending receipt of application to deregister must be dated or some source of authority recorded. There needs to be a trigger reconnection if no form received after a set period (See Process C4 - Process consumer deregistration from HealthConnect (BA v1.9 Specification p. 28.)

C-46 Once a HealthConnect solution has incorporated EHR information into a consumer’s HealthConnect EHR: (a) this information must not be deleted or altered; however, (b) the HealthConnect solution must allow the originating provider to submit corrections or amended information for inclusion in the EHR in the form of revised versions; and (c) the latest such revised version is to be used in place of any earlier versions and be accompanied by appropriate annotations. (BA v1.9 Specification p. 10)

While there is nothing wrong with the statement about keeping material after correction, enabling access to the original and using latest versions, the complete blanket on destruction is not necessary.

**Finding:** Retention policy does not take account of copies in the different layers of the system and access is used as a retention tool. Many transactions would be temporary and could be deleted with appropriate appraisal.

**Implement access privileges for all participants**

Access in the primary setting is well developed for both providers and consumers, but not for secondary users. Providers participating in HealthConnect will be obligated to abide by existing privacy legislation and by specific HealthConnect privacy protocols—including when they access and use information from consumer’s HealthConnect records, and when they add information to these records. “As part of registration with HealthConnect, providers will be required to sign an agreement that includes an acknowledgement that their access to consumer information through HealthConnect will only be for the purpose of delivering health services to the consumer” (BA v1.9 p.4). This is a very weak requirement, although there may be some enforcement/compliance applied.

C-101 Deregistration of an individual provider may follow: ...(c) the individual provider being otherwise unable to continue as a health service provider, including having been removed from a professional register for misconduct; or d) a determination by the HealthConnect governing body that the individual provider has failed to use HealthConnect in accordance with the HealthConnect rules. (BA v1.9 Specification p. 45)

Provider access to view a consumer HealthConnect EHR implies that the provider requires access to the information for clinical purposes: All access will be audited and providers may be requested to provide reasons for an access event (BA v1.9 p.32) “Providers once authorised will be able to access all parts of a consumer's HealthConnect EHR” (BA v1.9 p 32) Issue of sensitive information being released to inappropriate health service providers was addressed at some length in v0.9, but technically difficult to achieve. Deregistration bars access and use of HealthConnect.

*The monitoring of health extends to subsequent implementations including consumer health diary.* The consumer health diary information will not be available to providers as part of the consumer HealthConnect record, though
mechanisms for access when the consumer is present may be established (BA v1.9 p65).

HealthConnect will allow any registered individual provider acting on behalf of a provider organisation that has been authorised by the consumer to access the consumers EHR for the purpose of providing health services to the consumer (BA v1.9 p32). Issue of granularity of access within an organisation and the definition of what is defined as an organisation

H. Deliver consumer access to HealthConnect. Process H1 - Provide a HealthConnect consumer access portal to support consumer access to HealthConnect services including access to the HRS service on which the consumer's EHR is stored and the consumer registration system ( BA v1.9 Specification pp59-60).

HealthConnect states that stringent security and authorisation mechanisms will be put in place to ensure that only authorised providers can access consumer records. Different levels of authentication will apply depending on the access scenario. Access by a consumer is granted to an organisation not an individual provider (BA v1.9 p.32). In addition to registered authorised providers, a provider organisation may authorise other staff to access HealthConnect on its behalf (BA v1.9 p120).

“[Consumer] presenting their Medicare smartcard (or possibly in the future other HealthConnect smartcards) at the first presentation at a healthcare provider/organisation. … The consumer will not need to present their card at subsequent visits to that particular health care provider organisation. Alternative processes will be put in place in the absence of a smartcard” (BA v1.9 p 63). The process involves:

- Identification of consumer (implicit authorisation/verification - PIN and HealthConnect no.)
- Identification of provider (implicit authorisation/verification - PIN and HealthConnect no.)
- Verification of provider on consumer's access list
- Consumer identification, verification

Every access requires a record of the recordkeeping transaction - date, what accessed, who, when
- Access and view EHR (record of transaction)

- Access and view access log (record of transaction)

Reconstruction of consumer registration records at various points of time (*all changes are time identified and a particular view of the record at a specific time can be recreated* - needs authenticity checks)

**Finding:** Access in the primary setting is well developed for both providers and consumers, but not for secondary users.

**Maintain records of express and informed consent of consumers to both primary AND secondary users of HealthConnect records**

“The access control arrangements are without time limit and will remain in force until such time as the consumer changes them” (BA v1.9 p56). The proposal for indefinite continuation of consent needs social acceptance.

Agents can be appointed. It expands on the guardian concept in previous versions of the business architecture. An agent is a person nominated by the consumer to access his/her record on their behalf (BA v1.9 p31 and p53). Consent is limited to participate and to nominate primary users. Agreement to HealthConnect registration involves automatic acceptance of the inclusion of secondary uses. There does not appear to be an optional component to this. It is a blanket, continuing (even when participation revoked) authorisation “Consumers will be advised that consent to participate in HealthConnect will include consent for HealthConnect information to be used for approved secondary uses” (BA v1.9 p53 and p95).

The HealthConnect general principles ensure that a consumer (with legal capacity to deregister) has the right to deregister as a HealthConnect consumer at any time (see requirement C-17 BA v1.9 Specification p28). From a recordkeeping view the patient’s consent preferences are part of the record. Recordkeeping requirements include:

- Updates of EHR consumer registration and consent processes
- Updates need to have a record created.
- Verification of transmission of message or error messages for record integrity.
**Finding:** There is an inadequate consent model, with express consent only for the initial sign up and implied once the patient is in the system; the use of “standing consent” until one opts out and secondary uses assumed on registration and the shelving of more sophisticated approaches that would have placed restrictions on those who can access highly sensitive health conditions.

**Manage access by third parties which conforms with relevant laws and ethical codes**

*HealthConnect* has not fully developed the rules for third party access even though it has detailed processes for monitoring access. Consumer access does not cover secondary uses (see Process G3 - Retrieve/use EHR Information p. 59). Secondary users’ responsibilities are listed as: commitment to using information only for purposes stated, participation in line with *HealthConnect* confidentiality and privacy arrangements; commitment to abiding to *HealthConnect* processes and rules relating to circulating and publishing information and provision of a secure environment for storage of *HealthConnect* supplied information (BA v1.9 p96).

“Masking” specific health events or categories of data is a possible option for restricting access to specified health details, but technically difficult unless pre-determined categories are set. A UK model assumes a permission to share with persons who treat the patient. *HealthConnect* does not include this functionality at present (V 1.9, p. 55). As the EHR List contains active health problems it would be a contender for having some of its data “sealed” off.

Where there is a legal requirement for inaccurate data to be rectified/deleted a record’s integrity may be affected. This issue has to be resolved in data protection regimes. ‘Lapse of time’ archival principle is not given due weight in researcher codes of conduct which adopt privacy principles. Also there is the archival issue of preservation as part of primary rather than secondary use.

Patient amendment rights should not diminish a record’s integrity. Right of amendment should allow the right of a notation where patient disputes summary, or demonstrate inaccurate a right to delete it or mask it in case it is needed for litigation. “…the common law principle that rights to privacy do not diminish significantly over the lifetime of the individual to whom the information relates and

---


second, to the common sense principle that, in some cases, these rights are not extinguished even with the death of that individual."19

Finding: HealthConnect has not fully developed the rules for third party access.

LEGAL REQUIREMENTS AND PRINCIPLES (SELECTIVE)

Recognise record as process rather than as object in evidence law

Principle: The best evidence rule, that is, the production of an original record is the best evidence defines electronic records as products of processes.

The original record rule has been abolished in many common law jurisdictions, but does not completely detract from the need of either party in legal proceedings to prove that the record is what it purports to be, and that its identity and integrity have not been compromised. For example, Evidence Act 1995 (Cth) ss 146 and 147 relate to presumptions that enable documents, regardless of format, as long as they form part of the records belonging to or kept by a person, body or organisation in the course of, or for the purposes of a business, and that are produced by processes, machines or other devices that function properly, to be acceptable as evidence. The rationale is that if a business depends on electronic records they may be presumed to be reliable and authentic. The presumptions can be legally challenged. Records that have been migrated from previous systems in the normal course of business would most likely be accepted as authentic copies.

Ensure records have the capacity to be used as legal evidence.
See also comments above for: Recordkeeping Requirements: Comply with laws of the relevant jurisdiction

Recognise the legal implications of relying on incomplete records

Principle: Provider liability and indemnity for inaccurate shared health records

Liability arising from incomplete or incorrect information may give rise to damage claims by parties affected. Therefore to prove that incorrect information was provided there needs to be evidence of what was seen by the parties. The deletion of inaccurate personal information can in fact lead to the absence of evidence of the incorrect data used in further action. Rather than

19 MacNeil, p 79.
deleting the inaccurate data, a correction should be made via a notation system.\textsuperscript{20}

There are litigation benefits of a secure, unalterable record in the legal interpretation of “standard of care”. There is a legal risk for providers relying on an “incomplete record” or technology that does not deliver.\textsuperscript{21}

If the HealthConnect record is not a “complete” patient health record, should it be relied on at all for clinical decisions?

“All States of Australia (though not as yet in the Territories), professionals, including medical practitioners, are not liable in negligence if they act in a manner that is widely accepted in Australia by peer professional opinion as competent professional practice.” \textsuperscript{22} The accuracy, comprehensiveness and hence, reliability of HealthConnect records will be compromised to the extent health care providers choose not to opt-in.

**Ensure that event histories are defined as record in privacy and evidence law**

**Principle:** Privacy principle of individual control over collection, use and disclosure of personal information including health

See also comments above for: \textit{Explicitly recognise that audit trails (event histories) are part of the record}

It is not clear in Australian privacy law as to whether transactional data collected when a patient, doctor or researcher accesses the system is included in the meaning of personal privacy.

**Seek an interpretation of de-identified data and “potentially identifiable data” in privacy laws**

**Principle:** The privacy “Purpose Limitation Principle”

Non-release of third party of information provided in one context for another unless explicit consent given.

Although there are no general exemptions in Australian privacy legislation for access to personal information for historical, scientific, or statistical research,

\textsuperscript{20} Iacovino and Todd, p 110.


there is an exception for health information or temporary public interest determinations. Under the Privacy Act 1988 s 80A “temporary public interest determinations”, the Privacy Commissioner can make a Public Interest Determination allowing for derogation from a National Privacy Principle which could be requested for particular records regardless of age for research within specified guidelines. In the Privacy Act 1988 s 95A disclosure of health information for statistical or research purposes must comply with Guidelines prepared by National Medical Research Council and be approved by the Federal Privacy Commissioner.

Ensure doctors and other health care providers abstain from disclosing information imparted to them in the course of a professional relationship unless authorised by the patient or by statute.  
**Principle:** Medical and legal duty of confidentiality of doctors not to disclose information imparted to them in the course of a professional relationship

Right of confidentiality encourages frank disclosure of information by patient therefore is more likely to be reliable and accurate. There is a link between confidentiality and patient candour as accepted in case law and research. R v Department of Health; Ex Parte Source Informatics Ltd, [1999] 4 All ER 185 at 196 per Latham J.23

There are limitations on confidentiality through legal requirements for healthcare providers to disclose medical information for research, health reporting, health and insurance administration or litigation purposes.24 Even where disclosures are lawful patients expect to be informed if the information is not related to their treatment.25

Ensure consent to participate by the patient or provider is informed. Ensure consent by the patient to secondary of personal data is explicit  
**Principle:** Privacy requires informed consent from participants for the collection, use and disclosure of personal information and explicit consent for the release of information to third parties who are not involved in the provision of healthcare to them.

Unlike confidentiality, privacy is concerned primarily with an individual’s ability to exercise control over his or her own identifiable personal data. Privacy and the principle of patient autonomy both require the ability to exercise control over their

---

23 Paterson p 82.
24 Paterson p 86.
25 Paterson p 87.
personal information. The right to privacy has evolved from the notion of limitation of government control over individuals. Seeking of consent is an element of respect for the individual based on the principle of autonomy. In HealthConnect this requires that the consumer has the ability to restrict access to types of providers. There must be non-release to a third party of information provided in one context for another context unless explicit consent given.

Paterson distinguishes privacy from confidentiality and information security. Information privacy principles involve informed consent on purposes of data collection at the time of collection and subsequent uses and disclosures are to be consistent with those purposes. Privacy requires data security, but it is possible that a secure system does not give an individual control over disclosure of their personal information and therefore does not provide privacy.

Given the lack of consistency in privacy legislation in Australia, additional policy rules and/or legislation to deal with specific privacy issues relating to HealthConnect need to be developed (BA v1.9 p167). HealthConnect participants will be obliged to abide by privacy legislation and by specific HealthConnect 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 p78). As the implementation of HealthConnect is at present building on independent state-based electronic health initiatives, with each patient registered in only one HRS a patient whose EHR is in New South Wales may have a legal advantage over a patient whose record is in a state with no specific privacy provisions dealing with identifiers. It is envisaged that the complaints process will be based on current practices, with private sector privacy complaints being directed to the Office of the Federal Privacy Commissioner and public sector privacy complaints to the state or territory body authorised to deal with privacy and health complaints in each jurisdiction. This introduces different jurisdictions with potentially different rules, which depends on “ownership” or “location” of the service/data store.

**Ensure private sector contracts for HRS include all rights and obligations.**

**Principles:** Contractual liability must be the subject of an express or implied guarantee of truth (or falsity); vicarious liability of employer/contractor for employees who breach security; and duty of confidentiality and privacy rights to be included in contract.

---

26 Paterson p 80.
HealthConnect will devolve responsibility in many areas to private sector for security and should take account of vicarious liability for employees who breach security.

**Determine both statutory requirements and potential litigation needs in relation to retention**

**Principle:** Duty to preserve records before litigation commences.

Deletion principle in privacy laws may, in some circumstances, conflict with recordkeeping principles of reliability and authenticity.

Apply other legal requirements re: retention.

Records may be required in anticipation of possible litigation because the law implies an assurance that a person can make a claim within a time fixed by law, that is a limitation period which may in some circumstance be extended. District Court of South Australia, *Syrett v Vorbach*, No. DCCIV-99-336 [2001] SADC 46 (30 March 2001).

Records retention currently depends on legislative requirements in different Australian states, including archival legislation. *Sui generis* health records laws passed in Victoria, NSW and the Australian Capital Territory have provisions regarding retention of personal health information. For example, *Health Records Act 2001* (Vic), HPP 4.2 provides that a health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless permitted by law, or not contrary to a law. Information can be deleted related to a child once the individual attains twenty five years or in any case seven years after the last occasion on which a health service was provided to the individual. Health information held by other organisations is treated the same as other personal information in relation to retention.28

Draft National Health Privacy Code is an amalgam of current state and Commonwealth health privacy provisions. If it is applied by HealthConnect to the national database, then the NHPP Principle 4 Data security and Data Retention proposes that information related to a child can be deleted once the individual attains twenty-five years, or in any case seven years after the last occasion on which a health service was provided to the individual as found in the Victorian Health Records legislation (see HPP 4.2 above). Does the seven years apply to discrete data or to the patient’s whole record or history? Some health information may not need to be retained and is covered in disposition schedules issued by archival authorities based on triggers for removing particular types of medical information from the record. In terms of potential litigation most medical practices

28 Iacovino and Todd.
keep patient records even longer than seven years. Alternative phrasing for 4.2 (b) (ii) could be “seven years after the last interaction or encounter with the health system”, effectively for the normal expected lifetime of a person, plus 7 years. Alternatively, a longer period could be considered, for example “30 years after the death of the patient” which would be consistent with the Code’s definition of the end of privacy.

_Circumstances when an individual should be able to request deletion (as opposed to correction and masking of health information from his/her record._

The question as to whether data should ever be totally deleted (as opposed to being amended or annotated) and the scope of the circumstances in which such a course might be appropriate has arisen for consideration in the context of applications for amendment under freedom of information legislation. The freedom of information acts differ in the way in which they deal with expungement: for example, the Freedom of Information Act 1982 (Vic), implicitly allows for it using controlled authorised destruction by requiring the concurrence of the Keeper of Public Records where a correction or amendment “has the effect of deleting or expunging the information". At the other extreme the Freedom of Information Act 1982 (Cth), s 50(3) has been amended so as to preclude expungement. The general approach taken in Victoria and in those jurisdictions where the position is less clear is that deletion is generally inappropriate.

In most cases the information privacy rights of individuals can be substantially protected by adding an appropriate amendment or annotation and ensuring that this is provided to any person who accesses or makes use of the information for decision-making purposes. This ensures that individuals are protected from the adverse consequences of decisions based on incorrect data while preserving the historical integrity of the document. For example, the fact that incorrect data was relied upon may be relevant in the context of litigation for malpractice. Health Records Act (ACT) principle 7 provides for a record found to contain inaccuracies to be held separately from the ‘active’ record in use by the treating team.

On the other hand, there may be some circumstances where information is demonstrably wrong and, its preservation even with appropriate corrections or annotations may result in ongoing harm to the individual whose information has been recorded. In some such cases the relevant review bodies have required total expungement (see, eg _Re Foster and Victoria Police_ (1989) 3 VAR 110). Paragraph 6.7(a) of the code is apparently designed to deal with this contingency. However, it would be preferable that the code be supplemented with guidelines which make it clear that the potential harm which must be
included includes potential discrimination resulting from the making of decisions which may impact adversely on the individual.29

ETHICS REQUIREMENTS AND PRINCIPLES

Maintain control over personal data for patient autonomy through ownership of process
Principle: Ethical principle of autonomy

In modern bioethics, the principle of autonomy is generally used in the sense that individuals have the right to make their own decisions about their health and be free from interference in this regard.30

One of the key privacy platforms of HealthConnect is that patients have access to information held about them, can maintain control over how their information is used and to whom it is disclosed, and can contribute to and amend their own electronic health record. These principles need to take account of legal and ethical rights of access to medical information including the therapeutic exemption in medical records where the doctor may withhold medical data of potential harm to the patient.31 The principle of therapeutic privilege provides withholding personal information from an individual on the basis that if it is known it would cause mental or physical harm to the individual concerned.32 It is based on case law and medical codes of ethics; and also supports a different treatment for mental health information and non-disclosure outside of the primary zone of care. Even with the express consent of the patient it has been argued that a doctor should not have access to masked data in the summary record for reports to third parties not treating the patient.33

Minimise the harm that may result to a patient or provider if reliable and authentic records are not preserved over time.
Principle: Utilitarian principle in bioethics on minimisation of harm to patient.

Utilitarianism:
What harm (consequences) result to a patient or provider if a particular process does or does not occur?

31 Paterson p 87.
32 McSherry p 60.
33 Ibid, p 89.
Who are the stakeholders and how are they affected?
Is the process likely to be in the public interest and does this public interest outweigh the patients' rights?

Utilitarianism operates on the principle that the greatest good outweighs greatest harm.

Recognise that ethical duties require clear allocation of responsibilities to persons (juridical and natural)
Principle: Deontological principle of professional duties to client.

Deontology (duties and rules):
“...a deontological framework for ethical conduct 'holds that the rightness of an action is determined by whether it adheres to an appropriate moral rule, regardless of the consequences'”.

It also takes account of respect for the dignity of persons a principle that is found in most of the ‘caring professions’. It is both a negative norm in that it limits the way we act against persons but it is also positive, “treat himself and all others, never as a means, but in every case at the same time as an end in himself”.

Whose moral duty is it to ensure that the process takes place with appropriate safeguards?
Whose rights are affected by the process, patient or provider?
Are there any ethical codes that are relevant to ensuring that rights and obligations are clear in the process? (eg Ethical Codes of conduct for health professionals).
How do you balance the rights and duties of each person involved?

Recognise the ethical implications of relying on incomplete records.
Principle: A medical practitioner has an ethical duty to create a record at the time of each professional encounter with the patient.

See relevant professional codes of ethics and deontological approaches.

34 McSherry p 55.
Recognise the ethical implications of relying on records that have been altered or cannot be correctly identified.

**Principle:** Ethical intentions are evidenced by outcome, therefore evidence of intention or at least circumstantial evidence of intention, is essential to ethical action.

See virtue ethics and deontology and their interpretation of motives.

**Maintain control over personal data for patient autonomy through ownership of process**

**Principle:** Ethical principles include control over use and disclosure of personal information including health

Increase awareness of and respect for personal health information and types of harm that can befall patients when their health information is carelessly disposed of.

**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

**Ensure participants are morally accountable through records systems that capture their identity and competencies in relation to each and every role**

**Principle:** Moral principle of accountability for action in a specific time and place includes ethical motives for action.

*Virtue ethics*

Which personal characteristics are likely to make an individual act ethically? For example, honesty prevents fraud, fairness, respect etc. (ie selecting people with particular personalities to be involved in health professions).

Are those handling the system trained in ethics?

Are there appropriate mentors assist young health professionals?

Nurture the virtuous person that has a disposition to keep secrets.

See also deontology above

**Ensure parties to the contract act in good faith.**

**Principle:** Moral obligation to be truthful in contracts, that is, not to provide misleading information about what is intended in the contract. Other ethical
elements are fair conduct, unconscionable conduct and good faith in contract negotiation supported by case law.

**Protect the community from harm and provide for accountable actions in the public interest**

**Principle:** Ethical duty to preserve records before litigation commences and for accountable actions.
Duty to prevent harm in public interest (see utilitarianism above)

**Ensure patient has capacity to consent.**
**Ensure agents representing patients are appropriate.**
**Allow individual control/choice as moral agents.**
**Principle:** Respect for patient autonomy is not compatible with standing consent.

**Adhere to the moral duty of confidentiality re identified and de-identified data**

**Principle:** Respect for a person’s moral right to privacy

- Patients should retain maximum control of the uses and disclosures of their identifiable personal information.
- Secondary uses must take account of any harm to the patients whether identified or de-identified.
- Potential harm to an individual if information is accessed by someone who poses a threat to that person (eg domestic violence).
- Patients should be informed that their de-identified data may be used for research or other purposes.

The principle of autonomy requires that it should be up to the patient to decide who should have access to their personal health information. Disclosure of confidential health information to another health professional can be ethically justified on the basis that it is necessary if patients are to receive the full benefit of medical treatment. Consent to its use by researchers should not be presumed. A patient must be informed that third parties may access his or her records. 36

Archivists address confidentiality by assuming a lapse of time approach. Another issue is whether all EHR transactions will be confidential.

**Acknowledgment**
Barbara Reed’s analyses form the major part of the findings of the project.

---

36 McSherry p 55.
Main References


List of Abbreviations


Terminology

“Principles are statements that have general validity in a given sector or field. In applied sciences, they are conceptual statements on which a science, an
argument, or a reasoning is based, derived from the observation of individual facts.” InterPARES Project Strategy Task Force Report, p 2.

A requirement is more specific than a principle eg see IP1 benchmark requirements.

A policy is a formal statement of direction or guidance as to how an organization will carry out its mandate, functions or activities, motivated by determined interests or programs.

A strategy is the complex of practical means formally articulated by an entity for reaching a specific purpose, that is a plan or a road map for implementing policies.

A standard is the complex of established norms aiming to make the characteristic of a product, process, or service uniform within or across a sector, a country, or a system. In technical or industrial use, a standard is a model or a type of a given product. InterPARES Project Strategy Task Force, Report, p. 1, footnote 1.

Record-related Glossary of Terms

Authenticity
“Authenticity is established by assessing the identity and the integrity of the record. It must be possible to ascertain at all times what a record is, when it was created, by whom, what action or matter it participated in, and what its juridical/administrative, cultural, and documentary contexts were. It must also be possible to ascertain the wholeness and soundness of the record: whether it is intact or, if not, what is missing.” (InterPARES 2 Terminology).

Reliability
Reliability is the “trustworthiness of a record as a statement of fact. It exists when a record can stand for the fact it is about, and is established by examining the completeness of the record's form and the amount of control exercised on the process of its creation.” (InterPARES 2 Terminology).
HealthConnect Glossary of Terms


**Access control list** A list of provider organisations authorised by a consumer, or by a surrogate of a consumer, to access that consumer’s HealthConnect EHR.

**Access log** Record of access to EHR records (including emergency override access) by healthcare providers, consumers, HealthConnect registration agencies and HealthConnect system administration functions.

**Access portal** A computer system that provides users with a means of accessing an information system across the Internet using a web browser. Consumer access portals and provider access portals will be one means by which consumers and providers respectively may access HealthConnect functions.

**AEM Approved EHR Manager** A public or private entity authorised by the HealthConnect governing body to provide a HealthConnect Records System (HRS) service.

**Agent** Within HealthConnect, a person nominated by a consumer to access HealthConnect on behalf of the consumer. Also referred to as a “consumer agent” an agent is one form of consumer surrogate and would an appropriate form of arrangement to cover the authorized involvement of a consumer’s family members, friends, or carers.

**Aggregated data** Data about more than one consumer that are grouped together where the identity of the consumers cannot reasonably be ascertained.

**Attestation** The process of recording responsibility for a particular unit of information, such as a provider confirming the content of an event summary prior to its transmission to HealthConnect.

**Audit trail** A record of access and changes to information held in a computer system or database.

**Authentication** The process by which a degree of confidence is established about the truth of an identity. In terms of computer security, the identification or
verification of the eligibility of a consumer or healthcare provider to access a HealthConnect record.

**CEN** Comité Européen de Normalisation (European Standards Organisation) CEN 13606 The family of European Standards relating to electronic healthcare record communication.

**CIS Clinical Information System** A computer system designed to support healthcare providers in the delivery of healthcare. Examples include GP desktop systems, pathology laboratory systems and point of care clinical systems.

**Consumer** A general term used for a person who accesses or uses health services. Within HealthConnect, a ‘consumer’ or ‘participating consumer’ means a person that registers with HealthConnect as a consumer in accordance with the HealthConnect rules.

**Consumer consent** Agreement by an informed consumer to participate in HealthConnect or otherwise to authorise the collection or use of their personal information.

**Consumer index** Within HealthConnect, a database holding every HealthConnect consumer identifier, links to the HRS on which a consumer’s EHR is held, consumer demographics and other information that can be used to re-establish the HealthConnect consumer identifier, and information on providers and surrogates that may access the consumer’s EHR. The HealthConnect consumer registration service is responsible for maintaining the consumer index (through the HealthConnect consumer registration system) and for making information in the consumer index available to other HealthConnect services and components including consumer registration agencies, HRS services and message handling and translation services.

**Consumer registration agency** An organisation authorised by the HealthConnect governing body to register HealthConnect consumers in accordance with the HealthConnect rules.

**Consumer surrogate** A person (including a body corporate or partnership) that is uniquely identified to HealthConnect for the purpose of accessing EHR information on behalf of a consumer in accordance with HealthConnect rules. Identified subclasses of consumer surrogate include consumer agents, parents (for a child), persons with powers of attorney over a consumer’s health care, guardians of the incapacitated and any others recognised by the general law as having the right to act on behalf of the consumer.
De-identified data Data about a person or persons is termed ‘de-identified’ when the identity of the individual person or persons to which the data refers is not apparent, and cannot reasonably be ascertained from the data.

Deregister The process by which a consumer or provider discontinues their participation in HealthConnect. When a consumer deregisters, the consumer’s record is retained but made unavailable for further access by provider organisations and the consumer; information in the record remains available for secondary use.

eHealth access service A facility to give healthcare providers effective means of accessing HealthConnect services and any front line support needed to help them in using HealthConnect.

eHealth message bank service A facility for conveying eHealth messages between healthcare providers relating to any consumer registered with HealthConnect.

EHR Electronic Health Record A longitudinal collection of personal health information about a consumer, stored electronically. HealthConnect is Australia’s implementation of a national EHR.

EHR Extract The unit of communication of all or part of the EHR which is itself attestable and which consists of one or more EHR compositions.

EHR List A collection of similar EHR items describing a key aspect of a consumer’s health, formed to serve a specific purpose. An EHR List carries with it some notion of persistence, completeness, currency, maintenance, ordering. Examples include problem list and current medications.

EHR Notification A type of message or ‘flag’ sent to communicate important occurrences – usually specified in terms of a condition or set of conditions that when satisfied, triggers a pre-defined response. Examples might include hospital admission, emergency department attendance and hospital discharge.

EHR Report See report.

EHR Request An input transaction component sent to the EHR repository whenever users want to access data, and includes information such as the identity of the requestor, type of request (e.g., EHR view or request to enter/update data), the purpose of the request, and the EHR query itself.
**EHR System** Method for recording, retrieving, and manipulating information in electronic health records.

**EHR Transaction** An input or output from an EHR representing a single unit of activity on the EHR repository as a result of a provider’s interaction with the EHR.

**EHR View** A pre-defined set of data items selected from the EHR and returned in response to an EHR request.

**Encryption** Transformation of data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption).

**Enrolment** The process by which consumers, individual health providers and health provider organisations become participants of HealthConnect. Also see the preferred term: *registration*.

**Emergency override** The ability of personnel of a healthcare provider organisation to access a consumer’s HealthConnect EHR in an emergency situation where: (a) the consumer is unable to consent; (b) there is no one else available to give consent; and (c) the provider organisation is not already on the consumer’s access control list.

**Event summary** Within HealthConnect, information about one or more healthcare events, that is relevant to the ongoing care of a consumer and may be a subset of the information about the consumer held by the provider. The collection of health event summaries relating to a consumer forms the basis of the consumer’s EHR within HealthConnect. Proposed event summaries include some that contain information currently found in a specialist referral, hospital discharge summary or laboratory test report.

**Extensible** Sufficiently flexible to allow future changes that were not previously anticipated at the outset.

**Federation paradigm** The assumption that HealthConnect is to be implemented as a unity of potentially different HealthConnect Records Systems operating to common interface standards and supported by common services at a national level.

**Governance** The process of public accountability for the way in which an organisation conducts its business and may involve stakeholder representation and structures supporting responsibility, accountability and reporting.
Health record A repository of information regarding the health of a consumer. The health record may be paper-based or held electronically. See EHR.

Healthcare provider See provider.

HealthConnect governing body An entity on behalf of all the participating governments and other stakeholders with the overall management of the HealthConnect program at the national level.

HeSA Health eSignature Authority An independent subsidiary of the Health Insurance Commission that acts as a registration authority for the provision of digital keys and certificates required for public key infrastructure used within the Australian health care sector.

HL7 Health Level 7 Inc. A global standards development organisation that specialises in standards for information interchange between systems in the health care sector.

HRS HealthConnect Records System A computer system for storage and management of consumers’ EHR information and for controlling access to that information. The HealthConnect EHR repository is the sum total of the EHR information held by the HRS services.

HRS service The operational function that manages and provides access to HER information in an HRS.

Identified data Data are termed ‘identified’ when an individual’s identity is readily apparent, or can reasonably be ascertained, from elements of the record.

Identifier A universal number or code that uniquely identifies a person or other discrete entity.

Individual provider Within HealthConnect, a registered health professional that is registered with HealthConnect as an individual provider under the HealthConnect rules. Individual providers include medical practitioners, registered nurses, pharmacists and allied health professionals involved in the delivery of health services to individual consumers.

Initial health profile Summaries of a consumer’s previous health care (eg past medical history, family history and key pathology results) that form the initial entries in a consumer’s HealthConnect EHR.
**Metadata** Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted.

**National data store** A data storage and archiving service that aggregates EHR information from across all HealthConnect HRS services.

**National health identifier** A universal number or code that uniquely identifies each person at a national level.

**NEHTA National E-Health Transition Authority** Entity created to drive the national information management and information and communications technology priorities to June 2005, at which stage a longer term authority may be established.

**National health provider directory** A national repository of healthcare providers supporting several health care initiatives, including HealthConnect. See also provider directory.

**Provider** Within HealthConnect, a term encompassing individual providers and provider organisations.

**Provider directory** Within HealthConnect, a database holding details of every provider participating in HealthConnect, their HealthConnect identifier, and contact information that enables the provider to be contacted by various means including delivery or collection of eHealth messages.

**Provider organization** Within HealthConnect, an organisation that is registered with HealthConnect as a provider organisation under the HealthConnect rules. A provider organisation may be any business entity (including a sole trader in the case of an independent practitioner) that delivers health services directly to individual consumers. A provider organisation or other legal entity that provides health services may include other provider organisations. For example, a corporation that delivers health services may be registered as a provider organization and may comprise several regional hospital groups, each registered with HealthConnect as a provider organisation, and each of these may include hospitals and, below that, particular care teams, all registered with HealthConnect as provider organisations. Within HealthConnect, control of access to information within the consumer’s EHR is by provider organisation.

**Provider registration agency** An organisation authorised by the HealthConnect governing body to register HealthConnect providers in accordance with the HealthConnect rules.
**Registration** The process by which consumers, individual health providers and health provider organisations become participants in HealthConnect. Similar to enrolment.

**Report** Data from one or more EHRs designed to serve the needs of secondary users (such as clinical research or epidemiology reporting).

**Secondary Use** Any authorised use of a HealthConnect EHR other than for the purpose of supporting the direct delivery of healthcare eg clinical research, epidemiology, population health and health planning.

**Shared EHR** Those parts of a consumer’s health record that are made available to (and therefore shared) as part of the consumer’s EHR.

**Value-added services** Additional services, created due to a specific business need, that are packaged with the core services.

**VPN Virtual Private Network** The concept of using the internet or other 'public' carriers as transit for private network traffic, usually in encrypted form.

**XML eXtensible Markup Language** A language for organising and annotating data for interchange between disparate information systems.