

Privacy Policy
For the
NSW Health Electronic Health
Record Pilot Project

March 2006.

Privacy Policy for the NSW Health Health*e*link electronic health record pilot project

Table of contents

1. Introduction	3
1.1 What is the purpose of this document	3
1.2 Who is bound by this Policy.....	3
1.3 What is Health <i>e</i> link?.....	4
1.4 General principles of Health <i>e</i> link.....	5
1.5 Participation in Health <i>e</i> link.....	5
Consent and capacity for Health <i>e</i> link participants	6
1.6 Benefits of Health <i>e</i> link.....	7
1.6.1 Benefits to healthcare providers	7
1.6.2 Benefits to healthcare consumers	7
2. Health <i>e</i> link and Privacy.....	8
2.1 What is personal health information	8
2.2 Overview of privacy legislation	9
3. Compliance with Health Privacy Principles.....	10
3.1 Collection Principles HPPs 1 – 4	10
3.1.1 HPP1: Purpose of Collection	10
3.1.2 HPP2: Collection of information must be relevant, and not excessive, accurate and not intrusive.....	11
3.1.3 HPP3 - Collection from the individual concerned.....	12
3.1.4 HPP4 - Informing individuals about Health <i>e</i> link.....	13
3.2 Retention, security and protection Principle HPP 5.....	14
3.2.1 HPP5 Security of personal health information	14
3.3 Access and amendment Principles HPP 6, 7 & 8.....	19
3.3.1 HPP6: Ascertaining whether an organisation holds personal health information about you.....	19
3.3.2 HPP7 Providing access to the individual	19
3.3.3 HPP8 Amendment of Personal Health Information.....	20
3.4 Accuracy principle HPP 9.....	21
3.4.1 HPP9: Accuracy.....	21
3.5 Using and disclosing personal health information principles HPP 10 & 11.....	22
3.5.1 HPP10 & 11: Limits on Use and Disclosure of Health Information	22
3.6 Identifiers principle HPP 12	25
3.6.1 HPP12 Identifiers.....	25
3.7 Anonymity principle HPP13.....	26
3.7.1 HPP13 Anonymity.....	26
3.7 Miscellaneous principles HPP 14 & 15.....	27
3.7.1 HPP14 Transborder data flows and data flows to Commonwealth agencies.	27
3.7.2 HPP15 Linkage of Health Records.....	27
Appendix 1: Health <i>e</i> link privacy checklist	28

1. Introduction

1.1 What is the purpose of this document

This document is intended as a specific privacy policy document guiding all participants in the NSW Health *Healthelink* Pilot.

The policy provides a guide to the expectations that are placed on all participants involved in the management and use of the *Healthelink* system ie

- Healthcare providers
- Healthcare consumers / consumers
- *Healthelink* personnel or its agents

The document summarises the legislative framework and outlines the business processes adopted to ensure that personal information collected, stored, used and disclosed as part of the *Healthelink* electronic health record pilot program is managed in compliance with the Health Records and Information Privacy Act 2002 and the procedures and policies outlined in the NSW Health Privacy Manual (v2) 2005 which remains the primary document pertaining to health information privacy and NSW Health.

The objective of this policy document is to document the **baseline** compliance of *Healthelink* with privacy legislation.

This privacy policy outlines a variety of measures that will maximise the security and confidentiality of a consumer's information within *Healthelink*, while allowing access required by the individual and their healthcare provider(s).

1.2 Who is bound by this Policy

This policy applies to all people who work within the NSW public health system, including employees, contractors and other health service providers who, in the course of their work, have access to personal health information. These include:

- providers of health services such as doctors, nurses, case managers, visiting providers and allied health staff
- managers, administrators, clerical and service staff
- technical, scientific and laboratory personnel, including system administrators
- auditors;
- interpreters;
- volunteers;
- students;
- consultants, temporary and contract staff;
- persons providing any other health service provided by the public health system including nursing homes, hostels and group, homes, community health services, drug and alcohol services, allied health programs, dental and early childhood services, multi-purpose services, scientific and laboratory services and health promotion and public health services.

The policy and procedures apply to people whose employment is part time, temporary, contractual, casual or short-term. These include volunteers and people who do unpaid work either as community volunteers, or clinicians working or observing as research fellows etc.

Ensuring enforcement of policy

The *Healthelink* application is unusual in that it covers public and private organisations, and that the consent to collection and storage of information is managed distant from the point of collection of the information.

- All private sector providers seeking access to *Healthelink* will be required to enter into a contract prior to access being granted. This contract will set out provider rights and obligations and reinforce their obligations to comply with the general law and the specific policies governing *Healthelink*. Participating provider organisations will be expected to act when breaches of use and disclosure occur within their environment.
- All Area Health Services participating in *Healthelink* will comply with Department of Health policies and directives and specific *Healthelink* policies and procedures. Area Health Services will be expected to act when breaches of use and disclosure occur within their environment, in line with existing policies and procedures.
- *Healthelink* will report to a governance committee on issues of audit, complaint management and other matters which may arise during the pilot.
- Appendix 1 of this privacy policy contains a checklist that will assist participating healthcare providers to ensure they are managing privacy issues when using *Healthelink*.

1.3 What is *Healthelink*?

NSW Health¹ has a commitment to ensuring that the information supporting the provision of health care is readily available to authorised users when and where it is needed. The implementation of the *Healthelink* Electronic Health Record Pilot Project is an important step towards meeting that commitment.

Healthelink will:

- store summary health information in an electronic format;
- be comprised of summary or snapshot views of individual healthcare service events, collected from a healthcare provider's computerised medical record system after each service;;
- allow doctors and other health professionals within the pilot areas to access up-to-date information about their patients' health if those patients are participating in *Healthelink*;
- provide consumers with secure access to a summary view of their health information via a *Healthelink* helpdesk service or the Internet;
- be optional. Consumers and private providers will be able to choose whether they wish to participate in *Healthelink*.

¹ For the purposes of this policy, the terms 'NSW Health' and 'NSW public health system' are used to cover area health services, statutory health corporations (including Justice Health and the Children's Hospital at Westmead), affiliated health organisations listed in Schedule 3 of the *Health Services Act* and the Ambulance Service of NSW.

Health*link* is different to existing records (both e-records and paper based) in two ways. First, it is not a primary source record, but as noted above, is a summary of certain limited events. Primary source records will be maintained by the relevant health service provider. Second, Health*link* is not limited to a single area health service or service provider, but is operated by the Department of Health, providing means to link data from different providers, enhancing the quality and relevance of information available to participating providers and consumers.

The scope of the pilot is:

- adults 65 years and older living in the following defined postcode areas.
2320
2321
2322
2323
2324
- children 0 to 15 years living in the following postcode area(s);
2145
2148
2750
2150
2170
2560
2747
2770

1.4 General principles of Health*link*

Health*link* has a strong requirement to protect consumers' information privacy. However, the information in Health*link* must support the provision of health care and should therefore be readily available when and where it is needed to support good clinical care. Given the nature of Health*link*, the following critical principles apply:

- Health*link* has been established expressly for the primary purpose of supporting health care and treatment of individual consumers;
- Health*link* **does not** replace the need for a complete and suitably detailed primary healthcare record;
- As a health record access to Health*link* is restricted to the consumer and those persons involved directly in the provision of healthcare or directly related purposes.

1.5 Participation in Health*link*

Consumer participation in Health*link* is optional. While a Health*link* record will generally be automatically created for a consumer following their first presentation to a participating Health*link* service provider, they will be offered the opportunity to "opt out" of the system at any time. At the time of the first presentation the consumer is provided with detailed information in a format that they can understand which explains what Health*link* is and their options regarding their participation in Health*link*.

Privacy law requires that consumers are fully informed of how their personal health information may be managed within Health*e*link. Effective communication is also vital to ensuring that consumers are able to make informed decisions with regards to their participation in Health*e*link. Details are provided in Section 3.1 (Collection) of this policy.

After a consumer's record is created in Health*e*link, a 30 day 'cooling off' period applies to enable the consumer to make a decision whether to opt out of Health*e*link. A consumer can also opt out of Health*e*link at any time after their record is created.

30 day cooling off period

During the 30 day cooling off period, no information will be accessible to any authorised providers or the consumer and their associates – that is, the first message that initiated the registration will be stored by Health*e*link but that information and subsequent messages will not be able to be viewed by users until the 30 day period has expired. The 30 day period starts from when the initial message is received at Health*e*link. System administrators will be able to view the message at this point only as required for overall system maintenance and audit purposes.

If the consumer has not opted out during the 30 day cooling off period, at the end of that time their electronic health record will be automatically available to authorised providers and the consumer if he/she has registered for online access. Over time the record will build, through receiving event summaries from all visits to participating providers. Authorised providers, the consumer and their associates, will be able to access the record on an ongoing basis to support treatment and care.

If the consumer opts out at any point, their record will be automatically deactivated. Any information that has been collected up to the point of opting out will continue to be stored as an inactive Health*e*link record, but the record will not be accessible to any providers, the consumer, their associates etc. Records will only be accessible via the centralised Health*e*link administration for maintenance, audit and other purposes recognised under the privacy legislation.

Consent and capacity for Health*e*link participants

The HRIP Act establishes a test for capacity which states a person is incapable of giving consent if they:

- Cannot understand the general nature and effect of the matter they are being asked to decide on
- Cannot communicate their intentions about that matter.

When treating a minor, the treating healthcare provider should assess the maturity of the consumer, in particular their ability to understand the consequences of their decision. Where a consumer is less than 14 years of age, consent should generally be given by the parent or legal guardian. Where the consumer is 14 or older, if the treating healthcare provider does not believe that the child has capacity to decide for themselves, consent should be sought from an authorised representative such as a parent or guardian.

Except where special circumstances exist, parents will have control of their children's Health*link* records from 0 to 14 years including deciding whether the child participates, creating associates, opting a child out etc.

After a child turns 14 years old they will be able to manage their own Health*link* record, making their own decisions including the capacity to opt in, or out, associate or disassociate persons. Participating children approaching the age of 14 will be sent a letter six weeks prior to their 14th birthday advising them they will be able to manage their record as of their 14th birthday if they choose.

If a person does not have the capacity to decide for themselves, an authorised representative can give consent on their behalf. Health*link* allows authorised representatives (upon provision of appropriate evidence of identity and proof of the relationship) to have access to the participating consumer's Health*link* record, including decisions on whether to participate and adding or removing associates.

Further information: Privacy Manual, Section 5

1.6 Benefits of Health*link*

1.6.1 Benefits to healthcare providers

The primary benefit of Health*link* is in providing healthcare providers and consumers with quick access to a summary view of a consumer's health care history. Healthcare providers will have access to results, opinions and other healthcare information held by other healthcare providers looking after the same consumer. This has many positive implications including reducing the likelihood of missing critical facts when evaluating a consumer's healthcare requirement. Some specific benefits include:

- increased ability to provide safe, quality health care services, in emergency situations, especially where the consumer is unconscious and has had no previous contact with a particular facility;
- more complete picture of the consumer's health status;
- reduction of adverse events that may have occurred due to incomplete understanding of medical history;
- increased opportunities to be aware of and follow up on results or ongoing care, resulting in higher quality of health care;
- improved coordinated care both within the public sector and across the public and private sectors, leading to effective management;
- no need for duplication of tests, speeding up the ability to provide care, reducing costs, and resulting in a more efficient service;
- increased potential to identify safety issues for the consumer, other consumers and staff.

1.6.2 Benefits to healthcare consumers

Health*link* provides three key areas of healthcare benefits to the consumer:

1. Due to healthcare providers being able to access a wider range of relevant and up-to-date health information about the consumer, the

- delivery of more informed and therefore higher quality of healthcare is possible;
2. In addition, *Healthelink* provides consumers with a simple way to have important information from each healthcare service provided to them collected on their behalf and made accessible to them in one place free of charge.
 3. Consumers will have access to audit logs so for the first time they will be able to view which providers have accessed their record and what information they have viewed.

2. *Healthelink* and Privacy

The *Health Records and Information Privacy Act 2002* (the HRIP Act) governs the personal health information captured in *Healthelink*. The NSW Health Privacy Manual provides guidance to health services staff on how to comply with the requirements of the Act, notably the fifteen Health Privacy Principles, which govern all aspects of personal health information management.

The Act allows personal health information to be used by healthcare providers to support the provision of healthcare, where adequate system security is in place, and where the consumer has been made aware of how their information will be used.

As the Act protects the privacy of the consumer's health information, appropriate measures must be taken to ensure that the *Healthelink* system complies with the requirements of the Act. Users of the system will be required to access the system in ways which are consistent with the Act – for example, healthcare providers should only access relevant records of the consumer for whom they are providing health services, and when they need information for that ongoing care.

This policy was produced to ensure that the *Healthelink* system and users of the system comply with the HRIP Act.

The policy's requirements are designed to maximise the security and confidentiality of a consumer's information within *Healthelink*, while promoting authorised access when the consumer and/or their healthcare provider(s) require it.

NSW Health agencies however should be aware that the Commonwealth Privacy Act does bind non-government organisations and private sector health providers (such as individual medical practitioners and private hospitals), and so will be relevant to the way these organisations interact with NSW Health.

2.1 What is personal health information

Personal health information is defined as information or opinion about an individual whose identity is apparent or can reasonably be ascertained, and information or opinion about an individual's physical or mental health, health services already provided or to be provided to them, their health care wishes; it may also include information associated with the donation of body parts, organs and body substances, and genetic information.

By its nature, Health*elink* will contain personal health information and so the obligations under the HRIP Act will apply to Health*elink*.

2.2 Overview of privacy legislation

The *Health Records and Information Privacy Act 2002* (HRIP Act) and Regulation allows for the collection and storage of personal health information through a state-wide electronic health record in NSW, provided the requirements of the Act are met. These requirements relate to the collection, use, disclosure, access and security of personal health information held in Health*elink*. It is particularly important that all consumers are fully informed about Health*elink*, including the way their information will be used, stored and disclosed in the system, and their options to opt out of Health*elink* if they choose.

The pilot does not require express consent from a consumer prior to inclusion in the Health*elink* provided that:

- the consumer or their authorised representative, is made aware of the fact that their information is contained in a Health*elink* electronic health record, and what this means in relation to how their information will be used and disclosed
- the consumer, or their authorised representative, is given the opportunity to opt out of Health*elink*.

A basic principle of the Health*elink* program is that the consumer has the right to opt out of the program at any time if they wish.

The decision to opt out will not impact in any way an individual's right or access to health care services.

Relevant Laws and Policies

The 'Privacy Policy for Health*elink*' has been developed in accordance with various laws and policies, and as such is a guide to applying these laws and policies to the use and operation of Health*elink*. Detailed information about the HRIP Act is contained in the *NSW Health Privacy Manual (v2) 2005* and it is recommended that the manual be used as the main point of reference for information related to privacy legislation.

The 'Privacy Policy for Health*elink*' must also be read in conjunction with:

Privacy laws and policies

- NSW Health *Privacy Manual* (PD2005_593)
- Statutory Guidelines (Privacy NSW 2004a, 2004b, 2004c)
- Health Records and Information Privacy Regulation 2006 under the Health Records and Information Privacy Act

Available via the NSW Department of Health Privacy websites:

- <http://internal.health.nsw.gov.au/privacy>
- <http://www.health.nsw.gov.au/privacy>

Healthelink policies and documentation:

- Healthelink Security Policy
- Healthelink Complaints Policy (www.healthelink.nsw.gov.au)
- Healthelink Information Kit (www.healthelink.nsw.gov.au)

Privacy laws relevant to General Practitioners:

- Privacy Act 1988 (Commonwealth) available at www.austlii.edu.au/au/legis/cth/consol_act/pa1988108 and
- www.privacy.gov.au

3. Compliance with Health Privacy Principles

The HRIP Act imposes a set of 15 Health Privacy Principles (or HPPs) relating to all aspects of management of personal health information, including collection, use and disclosure, accuracy, security, and access. This part of the policy addresses each principle and explains the measures that Healthelink will adopt to ensure compliance.

3.1 Collection Principles HPPs 1 – 4

3.1.1 HPP1: Purpose of Collection

“Personal health information must be collected by lawful means and for a lawful purpose. The purpose must be directly related to, and reasonably necessary for, the organisation’s functions or activities”

The *Health Services Act 1997* sets out the key functions for health services, which are summarised in the Privacy Manual. Privacy law allows for the collection of personal health information for these purposes, and for purposes directly related to the health services’ core functions and activities.

Information is collected by Healthelink to provide for, and support, clinical care and medical treatment of consumers. Under the *Health Administration Act 1982*, this information is collected by the Department of Health rather than an individual Area Health Service.

Information is collected from Healthelink by medical practitioners and other health service providers in both the public and private health system, in order to allow them to provide appropriate care, treatment and diagnosis.

Healthelink is designed to make clinical information more readily available to consumers and their health service providers whenever and wherever it is required for healthcare purposes.

Further details: Privacy Manual, Section 7.1

3.1.2 HPP2: Collection of information must be relevant, and not excessive, accurate and not intrusive

“Reasonable steps must be taken to ensure that the personal health information collected is relevant to the purpose, is not excessive and is accurate, up-to-date and complete; and that the collection of the information does not unreasonably intrude on the personal affairs of the individual.”

There are two aspects to compliance with this privacy principle. Firstly, relating to the design of Healthelink, and secondly, relating to the input of information by healthcare providers.

1. Healthelink is designed in such a way that allows only for relevant information to be contained with it. In this regard, information collected will be similar to information collected in a paper based medical record, although Healthelink provides for greater safeguards to ensure only relevant information is collected and retained. The Healthelink application is designed to receive summary information of predetermined content and format. :
 - The content is restricted to information identified after consultation with healthcare providers and consumers as being directly necessary for care and medical treatment.
 - The format and content have been mandated by:
 - Use of a standard HL7 (an electronic messaging standard) message specification which determines what information can be sent by the health care provider source system to Healthelink, and
 - standard templates within the Healthelink application which govern what can be viewed in the application.
 - Each system providing information to Healthelink may only do so after a process of identification and mapping of suitable information from source to Healthelink has been established. Periodic reviews, by appropriate parties under strict control and under the oversight of the Strategic Information Management branch of NSW Health, will be undertaken for quality purposes. Regular reporting to the Healthelink governance committee will also occur.
 - Changes or additions to information types to be included in Healthelink will only be made having regard to the overall principle that the information is necessary for ongoing care and treatment.
 - Additionally, HealthTechnology will conduct regular and ongoing quality assurance audits on all incoming messages from systems providing summary information and the internal Healthelink repository for compliance with prescribed record/messaging content, accuracy and completeness.

2. Healthcare providers who are entering information into Healthelink online will be made aware of their obligations under this principle when receiving training in the use of the Healthelink system. Healthcare providers must only enter personal health information into Healthelink which is:
 - relevant to providing the individual with healthcare services,

- is accurate, up-to-date, and complete, and
- does not unreasonably intrude on the personal affairs of the individual.

This privacy principle applies to healthcare providers in relation to all personal health information collected and recorded by them in their own records as well as Healthelink.

Healthelink will collect a predefined set of summary data from each participating service provider organisation via their electronic medical record/management system using secure electronic message to carry the information to Healthelink. The data categories stored in Healthelink include:

- Consumers' personal details including name, address and date of birth
- Consumer Health diary containing, appointments, health questionnaires
- Appointments
- Health observations recorded by consumers and their service providers
- Family history
- Allergies and alerts
- Medications and immunisation
- Medical history
- Procedures
- A summary of each service/contact provided to an individual by:
 - Hospitals during admissions for treatment by means of a Discharge Summary
 - Outpatient and emergency departments
 - Community and allied health
 - General practice
 - Public dental clinics
 - Diagnostic results (pathology and radiology)
 - Documents such as assessments, discharge referrals and letters if electronically available.

Further details: Privacy Manual, Section 7.2

3.1.3 HPP3 - Collection from the individual concerned

"Personal health information must be collected from the individual it relates to, unless it is unreasonable or impractical to do so".

Information for inclusion into Healthelink will generally be collected in the same manner as information collected for the inclusion in a paper based record. Health services are bound by the Privacy Manual to collect personal health information directly from the individual concerned, unless it is unreasonable or impractical to do so. See Privacy Manual, Section 7.3 for further details.

Consumer information is provided to Healthelink in several ways:

- Directly from the healthcare provider's computerised record, known as a 'source system';

- Direct manual entry into Health*elink* by a healthcare provider or the individual consumer

Health*elink* is reliant on the practices of the source system organisation and that they comply with the requirements of the privacy legislation in this regard.

Further details: Privacy Manual, Section 7.3

3.1.4 HPP4 - Informing individuals about Health*elink*

“An organisation that collects personal health information about an individual from the individual must, at or before the time that it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the collection”

Health*elink* is required to take steps which are reasonable in the circumstances to make consumers (or their authorised representatives) generally aware of what information is collected, how it will be used, and their rights to access that information. Health*elink* will meet this obligation through

- Public media campaigns,
- Brochures and posters containing general information about Health*elink* and where further information can be obtained. These will be available through health service providers and Health*elink* registration agents.
- A letter and information kit that will be sent to newly registered participants informing them about Health*elink*. These kits will contain:
 - How the system operates;
 - What the record will contain and how the information will be used;
 - The fact that the system is voluntary and consumers can opt-out at any time
 - Instructions on how to “opt out” , and
 - Instructions on how to get access to their own record.
 - If the information pack is returned unopened/uncollected or is undeliverable, the person will be opted out as Health*elink* will consider that they have not been in a position to determine if they want to participate.
- Internet resources accessible through the Health*elink* and NSW Health websites providing information.
- Brochures translated into major community languages will be available, as well as access to interpreters.

Further details: Privacy Manual, Section 7.4

3.2 Retention, security and protection Principle HPP 5

3.2.1 HPP5 Security of personal health information

“Personal health information must be kept for no longer than is necessary and disposed of securely. It must be protected by taking such security safeguards as are reasonable in the circumstances against loss, unauthorised access, use, modification or disclosure, and against all other misuse.”

Security is a key aspect of *Healthelink*. In recognition of the different security issues which arise in relation to collection and storage of information in an electronic as opposed to paper based system, *Healthelink* will be subject to additional security policies and protocols, in addition to standard rules set out in the Privacy Manual and other relevant policies applying to paper based systems. The security principles within the HRIP Act require health services to protect information from loss, unauthorised access, use, modification and/or disclosure. The security of electronic information is also governed by *Circular 2003/47 – NSW Health Electronic Information Security Policy* and the NSW Premier’s Department *Circular No. 2004-06 Electronic Information Security – Certification to AS/NZS 7799*.

Healthelink System Security

How does information get to Healthelink?

Information about an individual will get into *Healthelink* either by

1. Secure messaging (computer to computer) from the healthcare provider’s local patient management system to the *Healthelink* system, or
2. Via direct entry either by a healthcare provider able to access the individual’s record or by the individual or their authorised representative.

Healthelink also maintains strict security procedures, which govern the technical processes around disclosure of a consumer’s record to healthcare providers.

The management of detailed audit trails, and regular auditing of provider access to consumer information, is an essential component to achieving a high level of security within *Healthelink*.

If a breach occurs, *Healthelink* will seek to apply penalties applicable under the HRIP Act and other relevant legislation.

Healthelink policies include rules for:

- Authentication of individual users before providing access to the *Healthelink* system
- Consent and registration of consumers
- Logging and auditing

In general these policies allow access to data when the security rules are met. That is, any authorised service provider or healthcare consumer who can electronically identify themselves or the *Healthelink* administrator can access a consumer’s record.

Health*link* security is supported by business rules and penalties for failure to comply with the business rules.

There is significant overlap between issues of use and disclosure of information in terms of privacy, issues relating to the security of Health*link* and security of electronic information in general. Approaches to security of Health*link* involve both technical and non-technical solutions. Each of these is addressed below.

Technical security systems/ processes installed in Health*link*.

Health*link* is protected from external hackers and unauthorised access on two levels: the network level and the application level.

Network Level

A suite of measures and policies will be used to prevent and/or detect hacker access on a network level.

- All network devices and servers in the data centre have been built according to the "Centre for Internet Security" benchmarks (CIS).
- The Health*link* application will be protected by DSD EAL2 rated firewalls. In addition, the physical layout of the data centre follows a layered three-zone approach for advanced intrusion protection: Demilitarised Zone/web server zone, application server zone, and database zone. Each zone is separated from the other by firewalls and access control devices. All core clinical data is held in the third zone, the database zone.
- The data centre network and all servers are monitored by an intrusion detection system that logs and monitors all activity. A correlation engine collects the data from various points in the network and detects access patterns that potentially relate to attacks. Once a potential attack has been detected, operations staff is notified and access is automatically blocked as required.
- To protect data that is travelling to and from Health*link*, all communication (in particular communication via the Internet) is encrypted by SSL and/or PKI using certificates of recognised Certification Authorities.

Application Level

On the application level, the following measures and policies will be employed to prevent unauthenticated and unauthorised access.

- Authentication of users is performed through username and password.
- User Accounts are only issued to consumers and providers that have passed an identification process
- All data communicated via the internet (including username and password) is protected by strong encryption.
- Penetration tests will be performed on a regular basis to verify that no unauthenticated access to the application is possible.

Security Model

Once a user is authenticated, Health*link* applies a strict security model to prevent unauthorised access. The security model is based on user groups and restricts

access via a user group model that restricts functional access. Each user is a member of a specific group based upon their business role in the system. Group membership determines the functional areas to which the user has access.

Auditing

All access to the system will be audited on a functional level, recorded in an audit log and monitored by operations staff. Consumers will have access to this Audit Log to review all access to their record.

Auditing user access to Health*elink* documents is a fundamental part of ensuring that the privacy of consumers' personal health information is maintained. The Health*elink* application provides access to security information for auditing purposes and regular auditing will occur through these processes:

- tracking of activation attempts by unauthorised users – this provides information about the user, date and time of the attempt, identification of the document where access was attempted and, whether the attempt was successful.
- details of users that have accessed a particular consumer's Health*elink* record and the date/time of that access.
- A high level summary audit trail is available to users within each Health*elink* electronic health record. More comprehensive auditing reports will also be regularly conducted and checked for inappropriate access and use of Health*elink*.

A detailed audit policy will be implemented including a process for random auditing of access to a cross section of consumer records. The Health*elink* governance committee will receive quarterly audit reports.

Further information relating to the technical security systems established within the Health*elink* is provided in the Health*elink* Security Policy.

Non technical business approaches to support security in the Health*elink* system

Fundamental requirements for managing Health*elink* system access in terms of privacy legislation include the following:

- all AHS personnel must be familiar with the Health Privacy Principles contained in the HRIP Act
- all AHS personnel must sign a confidentiality agreement, prior to being granted access to Health*elink*, outlining the specific responsibilities regarding consumer privacy and the consequences of any breaches
- each user will be allocated a unique identifier (e.g. user name & password) for accessing Health*elink*.
- Login time-out settings have been incorporated into the Health*elink* solution.
- Health services registered to access Health*elink* must have measures in place to minimise the risk of inadvertent breaches of privacy (e.g. computers not in places of public access)

- System access will be terminated promptly when personnel cease employment with the organisation through which they gained authorised access.
- Processes for managing unauthorised access and/or breaches of privacy by appropriate means.

Monitoring for privacy breaches

The Health*link* operation is supported by a variety of business processes to reduce the risk of security breaches. These include:

- Auditing of transactions and reviewing these regularly and on an ongoing basis for patterns that may indicate misuse
- Policing complaints about improper data use
- Only granting access to authorised healthcare providers employed by participating healthcare facilities and Area Health Services, and to consumers after an appropriate evidence of identity process
- Making audit logs available online to consumers
- Ensuring a secure physical environment including intrusion detection, and procedures in place for immediate response.

Making Health*link* users aware of their obligations under privacy law

All personnel who are granted access to Health*link* information should be informed, and regularly reminded, of their responsibilities to consumer privacy and confidentiality. Health*link* will do this in a number of ways:

- Through messages posted within the application itself at login
- Through agreements with the employer health service to ensure that staff understand their obligations to privacy and confidentiality and that each Health*link* user has signed an access agreement and undergone training prior to being given a username and password.
- Through individual agreements with General Practitioners registered to use the system

Patient searches

Conducting patient searches has the potential to reveal personal health information that is not relevant to the search requirements. As this a potential source of inadvertent breaches of privacy, particularly in the case of treatment by specialist health services, measures have been undertaken to minimise this risk. For example, initial search functions will not reveal any more information than is needed for positive identification of a consumer's record.

Printing

Care must be taken when printing documents containing personal health information from Health*link* to minimise the risk of unnecessary disclosure of this information.

Personnel should observe the following guidelines to minimise such risk:

- the security of the information printed is the responsibility of the person printing it
- printing of personal health information should be on a needs basis

- care must be taken regarding the location of the printer used, in order to minimise the risk of unauthorised persons gaining access to the information
- printed documents should be considered a 'copy' and appropriately destroyed when no longer required
- where handwritten amendments or notes are made which are relevant to care and ongoing treatment decisions they should be entered into the Health*e*Link record as soon as is practicable to ensure Health*e*Link is kept accurate and up to date

Personnel must be made aware that auditing of logs and history files on printing activity will be available to Health*e*Link system administrator/s.

Privacy education

- All personnel are to be informed, and regularly reminded, of their responsibilities to consumer privacy and confidentiality.
- All training on the use of the Health*e*Link system is to include details of the security and privacy requirements for users.
- Participating health services have internal policies and protocols to support adherence to the health privacy principles as well as an undertaking to maintain individual privacy/confidentiality agreements with individual staff.

Confidentiality agreements

- All Health*e*Link users will be required to sign a confidentiality undertaking with their employer outlining the specifics of their responsibility regarding consumer privacy and consequences of any breaches. This requirement can be accommodated within the existing arrangements between employer and employees for Health information privacy generally.
- Each participating organisation will be required to hold such undertakings with their employees (who have, by association with that service provider organisation access to the Health*e*Link application)
- As the Health*e*Link administration will not have direct management responsibility over the majority of Health*e*Link users, the participation of health services will be dependent on the presence of internal policies and protocols to support adherence to the privacy principles as well as an undertaking to maintain individual privacy/confidentiality agreements with individual staff. This must be supported with a process to take action whenever breaches occur.

Management of breaches of use and disclosure

- The Health*e*Link administrator will monitor inappropriate access, and act on breaches of access as stipulated by the relevant legislation.
- Breaches of privacy/confidentiality will be treated seriously and Health*e*Link will seek to apply any penalties applicable either under legislation or within contractual agreements between participating organisations and their employees.

Further details: Privacy Manual, Section 9

3.3 Access and amendment Principles HPP 6, 7 & 8

3.3.1 HPP6: Ascertaining whether an organisation holds personal health information about you

“An organisation that holds health information must take such steps as are, in the circumstances, reasonable to enable any individual to ascertain

- *Whether the organisation holds health information relating to the individual, and*
- *If the organisation holds health information relating to that individual, the nature of that information, and*
- *The main purposes for which that information is used, and*
- *The person’s entitlement to request access to the information”*

All healthcare consumers who are registered into the system will be sent an information pack that outlines:

- what information is held in Healthelink
- the purposes for which the information is used
- methods to gain access to the information

This information will fulfil Healthelink’s obligation to this privacy principle.

Direct mail out will be supplemented by other means, including:

- Information about Healthelink on the internet and in participating health services and relevant local organisations;
- A 1800 number to support consumer enquiries about Healthelink generally and access to their record if they wish.

3.3.2 HPP7 Providing access to the individual

“An organisation must, at the request of the individual, provide them with access to their personal health information without excessive delay or expense. An organisation is not required to provide access where the organisation is lawfully authorised or required not to comply.”

The right of the consumer/client to have access to the personal health information held about them is a fundamental right under the HRIP Act and the NSW Freedom of Information Act 1989 (FOI Act).

Access may however be refused in certain limited situations. The right to refuse access in limited situations is recognised under both privacy laws and the FOI Act. This covers a situation where access places any person at risk of harm, including where the consumer’s mental or physical health may be affected or where others may be placed at risk.

Consumers who have applied for and gained a user name and password are able to obtain web-based access to their Health*elink* record at any time. Where a consumer has not sought a username and password, they may access their record via the Health*elink* administration

Information collected at the time of enrolment in Health*elink* and for the first 30 days after enrolment is not available to healthcare providers or the consumer. If a consumer does not opt out before the end of the 30 day cooling off period, clinical information will continue to be collected and added to that Health*elink* record from all future consultations with participating healthcare providers.

While consumers have considerable control over access to the record NSW Health acknowledges that there will be circumstances when it may not be appropriate for the consumer to have access to Health*elink* and this responsibility may need to be restricted or overseen by another party² such as a guardian or healthcare provider. In these circumstances an authorised representative may be provided authority to set access to the consumer's record.

Before providing such a party access the Health*elink* Administration will require either;

- documentary evidence of the individual's own identity and supplementary documentary evidence of the relationship to the individual; or
- the consent of the consumer to whose record the third party is being given access.

As with paper record systems, situations will arise where access may be refused. In particular, where access to medical or psychiatric information may have an adverse impact on the consumer, consideration may be given to refusing access. Health*elink* also reserves the right to deny access in cases where there are reasonable grounds to believe access may place another person at risk, or there have been allegations about misuse of access rights.

3.3.3 HPP8 Amendment of Personal Health Information

"Individuals may request that their personal health information be amended to ensure that it is accurate, relevant, up to date, complete and not misleading".

Health*elink* substantially enhances both consumers' and healthcare providers' capacity to manage the accuracy of the health record.

- Consumers will be able to add notes or information to their record identifying where they think there is a mistake or an omission. These notes will then be accessible to clinicians providing them with care.
- While consumers will not be able to directly amend information about them which has been entered into Health*elink* by healthcare providers, consumers will be able to apply for an amendment to personal health information held about them if they believe it is not accurate, relevant, up to date, complete or is misleading.

² NSW Health Privacy Manual 2004, 5.6 pp 14 - 15

- Healthcare providers will not be able to change consumer entries.
- Where there are issues with the content of a particular summary record a consumer or clinician may request an amendment to that record entry. A record of requests for amendment will be held by Health*elink* and refusals/concerns over action taken will be subject to an internal review by Health*elink* (not the service provider) as the holder of the record and agency responsible for meeting the patient's requests for amendment.
- The actual amendment of the Health*elink* record will be made by the Health*elink* system itself processing the updated message from the healthcare provider's source system.
- Service providers will, under their contracts, be required to comply with the Health*elink* and NSW Health Privacy Manual requirements on amendment. In responding to any requests generated through Health*elink* for an amendment, the healthcare provider is acting as an agent for Health*elink*.
- In the event there is a dispute over amendment, it should be dealt with in accordance with the relevant privacy law via an internal review or through reference to the relevant Privacy Commissioner.
- This process will ensure that Health*elink* and the primary record held by the service provider are in alignment. Where the clinician/source system organisation identifies an error in a record which has been used to populate Health*elink*, the source system will, following an amendment/update of its own electronic record, send an updated summary record to Health*elink*, creating an updated/amended version of the record entry in Health*elink*.

Further details: Privacy Manual, Section 12

3.4 Accuracy principle HPP 9

3.4.1 HPP9: Accuracy

Organisations must take reasonable steps to ensure that the personal information they hold is relevant, up to date, complete and not misleading.

Accuracy of information is critical to the operation of Health*elink*. At an application level, Health*elink* has adopted a number of strategies to maximise the accuracy and quality of the information held within the individual's record. These include:

- Use of standard templates for data entering the system whether electronically from source systems or manual directly into Health*elink*;
- Automated validation process that forces information being entered into the system to adhere to standard field formats or code sets;
- Validation of all incoming electronic information for compliance against agreed message standard, missing data and incomplete records;
- Application of logic checks to assess incoming information against information already in the record, eg a male having a pregnancy.

Furthermore, these will be supported with an ongoing quality assurance program managed by the Health*elink* administration that will:

- Conduct regular audits of the repository for data quality issues such as compliance with reporting standards, receipt of incoming messages etc.
- Review the compliance and performance of individual source systems and where necessary liaise with the administrators of source systems to resolve issues.
- Review and update codes and code sets to comply with relevant standards and Department of Health requirements.
- Monitor and identify quality issues generally and devise strategies to effect change to ensure information is both collected and interpreted accurately.

Further details: Privacy Manual, Section 10

3.5 Using and disclosing personal health information principles HPP 10 & 11

3.5.1 HPP10 & 11: Limits on Use and Disclosure of Health Information

For further details on all exemptions relating to the use and disclosure of personal health information, readers should refer to the Privacy Manual, Section 11.

“An organisation that holds personal health information can use or disclose the information for the following purposes

- *for the primary purpose for which the information was collected*
- *for other secondary purposes which are related to the primary purpose*
- *for purposes authorised by other laws (NSW Health 2005: 27–40).*

As with all personal health information held by NSW Health, privacy law imposes limits on how the information held in *Healthelink* can be used and disclosed. The rules for use and disclosure are generally the same.

Primary purpose

The primary purpose of the personal health information held in *Healthelink* is to provide health care to the individual and provide that individual with access to their own health information. *Healthelink*'s purpose is to provide a system to manage a consumer's information to optimise the provision of health care to the consumer. Whilst this purpose is intrinsic to the primary purpose of collection, *Healthelink* is not essential to the provision of healthcare to the consumer, and therefore does not fall into the category of 'primary purpose'.

Secondary purposes

The Act lists a number of secondary purposes for which personal health information can be used and disclosed, and are addressed here in relation to *Healthelink*.

1. Use and disclosure for a directly related purpose

Use and disclosure of personal health information is permitted where the purpose of collection of this information is directly related to the purpose of the use and disclosure, and where the individual would reasonably expect the use or disclosure.

As the purpose of *Healthelink* is to facilitate the provision of efficient, comprehensive, and quality healthcare, the purpose of *Healthelink* is directly related to the purpose of why the personal health information contained within *Healthelink* has been collected.

Use and disclosure of personal health information held in *Healthelink* is permitted where it is necessary for the administration and management of the system. For example, disclosure of personal health information to *Healthelink* administrators and users is permitted where it is directly related to the functions of *Healthelink*, such as quality assurance activities, auditing, complaints handling, or managing legal claims. *Healthelink* policy does not permit the use or disclosure of personal health information for any commercial purposes, or for disclosure to insurance companies, employers or any other group seeking to use *Healthelink* for pecuniary gain.

Prior to the disclosure of any information contained in *Healthelink* to administrators and users, a process of validation of identity and justification of need to access *Healthelink* is required. Access requires authentication with a username and password entered at each entry to the *Healthelink* system. User activity in *Healthelink* will be monitored by regular audit.

It is the responsibility of the senior officers responsible for the administration of *Healthelink* to ensure that *Healthelink* administrators and users are made aware of the requirements of this privacy policy.

2. Use and disclosure with consent

Use and disclosure of personal health information is permitted where the individual has consented to the use or disclosure. This allows for individuals to consent to a variety of additional ways in which their personal health information can be used and disclosed within *Healthelink*.

In addition, access may be provided to other persons or agencies where authorised or if required by law. See Sections 3 - 11 for further details.

3. Use and disclosure to prevent a serious and imminent threat to health or welfare

NSW Health may use or disclose personal health information if there are reasonable grounds to believe that the use or disclosure of personal health information contained within *Healthelink* is necessary to lessen or prevent:

- a serious and imminent threat to the life, health or safety of an individual
- a serious threat to public health or public safety

Further details: Privacy Manual, Section 11.2.3

4. Use and disclosure for management, training or research activities

The NSW Privacy Commissioner has issued statutory guidelines on the use and disclosure of personal health information for the secondary purposes of health services management, training and for research (Privacy NSW 2004a, 2004b, 2004c).

Further details: Privacy Manual, Section 11.2.4

5. Use and disclosure to find a missing person

NSW Health may use or disclose personal health information if the information is to be used by a law enforcement agency to ascertain the whereabouts of a missing person. This exemption only applies if the person has been reported to the police as missing.

Further details: Privacy Manual, Section 11.2.5

6. Use and disclosure to investigate and report wrong conduct

NSW Health may use and disclose personal health information if the health service has reasonable grounds to suspect that there has been or there is the possibility of unlawful activity, unsatisfactory professional conduct or professional misconduct. Disciplinary policies should be followed when using or disclosing personal health information for these purposes.

Further details: Privacy Manual, Section 11.2.6

7. Use and disclosure to law enforcement agencies, including police

NSW Health may use and disclose personal health information to law enforcement agencies where the disclosure is reasonably necessary to the functions of the law enforcement agency, and there are reasonable grounds to believe that an offence may have been or may be committed.

Further details: Privacy Manual, Section 11.2.7

8. Use and disclosure to investigative agencies

NSW Health may use and disclose personal health information if this is reasonably necessary to the complaint handling or investigation functions of an investigative agency.

Further details: Privacy Manual, Section 11.2.8

9. Disclosure on compassionate grounds

NSW Health may disclose personal health information to an immediate family member for compassionate reasons. This is likely to apply either in emergency situations, or where a person has died. Note that this exemption is the only one which applies only to “disclosure” and not to “use”.

Further details: Privacy Manual, Section 11.2.9

10. Use and disclosure authorised by law

NSW Health may use and disclose personal health information where this is allowed by or required by another law. Some common examples are:

- Disclosure to the Department of Community Services under the *Children and Young Persons (Care and Protection) Act*
- Disclosure to a court to comply with a search warrant or subpoena
- Disclosure to Workcover to comply with the *Occupational Health and Safety Act*
- Notification of infectious diseases and other statutory reporting under the *Public Health Act*

Further details: Privacy Manual, Section 11.3

11. Use and disclosure as required by the Minister or Premier

NSW Health may use or disclose personal health information if the information is required by the Minister or Premier.

Further details: Privacy Manual, Section 11.3.14

3.6 Identifiers principle HPP 12

3.6.1 HPP12 Identifiers

“Identifiers can only be assigned to individuals if this is reasonably necessary for the organisations to carry out any of its functions efficiently”.

The allocation of identifiers to individuals is essential for the safe and efficient management of *Healthelink*.

Healthelink will allocate a unique number to all individuals for whom it holds a record. This number will be used with other demographic items such as name and address as the basis of identification and matching of records belonging to the same individual and thus ensuring accuracy of the information. The allocation and use of this number is critical to the efficiency and effectiveness of the matching process and therefore the quality and safety of the consumer’s health information.

Healthelink will also utilise the State Unique Patient Identifier (SUPI) facility. This facility will match each record against known clients using a variety of criteria and if known will append their identifier to their record to enable accurate matching. If the consumer is not already known to SUPI a unique identification number will be created. The purpose of this practice greatly mitigates the risk of mismatching within the *Healthelink* application while facilitating the alignment of disparate information held about a consumer within the NSW Health system.

“If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either

1. *adopt its own identifier of an individual, an identifier of the individual that has been assigned by the public sector agency, or*

2. *use or disclose an identifier of the individual that has been assigned by the public sector agency.”*

Private sector agencies participating in Healthelink will be required to access and use consumer identifiers as part of their access to the system. They will also be required to provide a local identifier to Healthelink with the information about the health service. The presence of these identifiers reduces the risk of mismatching an individual's information with an incorrect record.

The identifier assigned to an individual's record can be passed back to the private provider's system so that subsequent records about that individual will come with the Healthelink identifier already attached.

Further details: Privacy Manual, Section 13.1

3.7 Anonymity principle HPP13

3.7.1 HPP13 Anonymity

“Provided that it is lawful and practicable, individuals should be given the option of not identifying themselves when dealing with health organisations”.

Healthcare consumers who choose to have anonymity in their dealings with Health Services will not have these services included in their Healthelink record if they have one. To append information onto a Healthelink record the record must contain enough information about the individual to identify them and match their information to the correct record – it is not practicable to participate in Healthelink while seeking healthcare anonymously.

Those wishing to be anonymous in their dealings with health services will be advised to opt out of Healthelink. Consumers may also opt out of Healthelink prior to a specific consultation and then opt back into the system after that consultation if they do not wish information from that consultation to be appended to the record.

Healthelink has the capacity to include information in the record when the healthcare consumer uses an alias, and that alias is known to Healthelink. If Healthelink is able to match information from a consultation where the consumer has used an alias to the Healthelink record of a participating consumer, the information will be added to that consumer's record. If a match cannot be made, a separate record will be created using the details of the alias. If a consumer does not wish information from consultations sought using an alias to be appended to their Healthelink record, they should opt out.

Further details: Privacy Manual, Section 8

3.7 Miscellaneous principles HPP 14 & 15

3.7.1 HPP14 Transborder data flows and data flows to Commonwealth agencies.

Privacy law permits the transfer of personal health information outside NSW where equivalent privacy policy exists. Currently all Australian states and territories have equivalent policy. Health*link* will comply with HPP 14 in accordance with the standard obligations under the Privacy Manual (see section 13.2).

3.7.2 HPP15 Linkage of Health Records

“Personal health information must not be included in a system that links health records in one service with health records in another health service unless the individual it relates to has expressly consented”.

A specific regulatory exemption from HPP15 has been provided for the Health*link* pilot. Whether this exemption should be retained after the end of the pilot will form part of the pilot evaluation.

The regulation provides for the use of an “opt out” consent model. This ensures health consumers will continue to be able to exercise the choice as to whether or not they participate in Health*link* and to exercise this choice at any time.

Appendix 1: Health*link* privacy checklist

- Are consumers informed about what information is collected in Health*link* and how it will be used?
- Are personnel informed of their responsibilities to consumer privacy and confidentiality?
- Do personnel have access to the NSW Health Privacy Manual?
- Have personnel signed a confidentiality agreement prior to being granted access to Health*link*?
- Does the agreement outline responsibilities regarding consumer privacy and the consequences of any breaches?
- Is each user allocated a unique identifier (e.g. user name & password) for accessing Health*link*?
- Have appropriate log in time-out settings been defined?
- Are processes in place to ensure that a user's system access is terminated promptly when employment ceases?
- Are processes in place to ensure that a user's system access is modified promptly if their employment conditions change?
- Are processes in place to audit unauthorised Health*link* access?
- Are processes in place for random auditing of consumer records?
- Are there processes in place to allow for specific auditing of access to Health*link* of those people considered to be at higher risk of breaches of privacy?
- Are breaches of privacy detected through auditing managed appropriately?
- Are search functions configured to minimise the amount of information revealed unnecessarily?
- In general is printing of information from Health*link* minimised?
- Do printed pages include a footer advising "Privacy notice: This document is confidential – please destroy appropriately after use" or similar warning?
- Are secure printers available in situations when printing is unavoidable?
- Are personnel discouraged from making handwritten amendments or notes on printed material from Health*link*?
- Is there a process for auditing logs and history files on printing activity?