



Health Informatics Society of Australia

Submission on Privacy in Health Information

Presented to the

Australian Law Reform Commission

**Response to the Australian Law Reform Commission's
Discussion Paper 72 - Review of Australian Privacy Law**

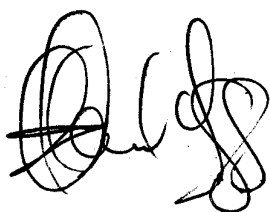
December, 2007

**Author: Prof Peter Croll
Professor of Software Engineering
Faculty of Information Technology
Queensland University of Technology
Director, Health Informatics Society of Australia**



Health Informatics Society Australia Ltd.

This document has been reviewed and represents a formal submission from the Health Informatics Society of Australia



Dr Michael Legg, PhD FAICD FAIM FACHI
MACS(PCP)

President,
Health Informatics Society of Australia

Opening Comments

Issues relating to privacy protection have been very active over the past year, both across Australia and Internationally. None more so than the area of health where the balancing act between ensuring patient confidentiality against dependable access by primary and secondary health data users proves most demanding. Advances in technology continue to challenge our ability to foresee the future, yet this technology has such potential to improve our quality of life in regards to knowledge and health care provision.

I am delighted that my colleagues in the Health Informatics Society of Australia have been so active and supportive in this crucial area. The results of several health privacy surveys, forums and discussion groups have helped in formulating this submission for the ALRC. It comprises a non-exhaustive list together with supportive commentary highlighting areas of concern that have been raised consistently through the many avenues of consultation. Unlike some of the funded national bodies we do not have a particular agenda to push through other than to represent the views and concerns of our members. That is, the majority of HISA members are more on the receiving end of state and national initiatives. Hence, I am pleased to see a significant consensus has been reached on key issues affecting health data privacy and security. I wish to thank all those that have contributed and hope that this submission will provide a valuable insight to what are complex yet essential issues that need to be addressed to ensure Australia remains at the forefront of medical knowledge and health care provision.

With best regards,



Professor Peter R Croll
Chair HIPS (HISA's Privacy and Security Forum)

Contents

Key Points / Executive Summary	5
Background.....	7
Commentary	10
1) National Consistency	10
2) Capabilities of Human Research Ethics Committee (HREC)	11
3) Wider Stakeholder Involvement	12
4) Maintaining Technology Neutrality	14
5) Towards ‘User-Centric’ Health Provision.....	15
6) Pragmatic Approaches to Consent Issues	17
7) Recognition of National and Globalisation trends with Health Data	20
8) Support for Clinical Audit and Quality Assurance.....	21
Comments from the HISA Survey	26

Key Points / Executive Summary

1) **National Consistency**

The majority of the HISA members seek national consistency with the proposed privacy laws across both the State/Federal and Public/Private sectors. The current proposals do not go far enough to resolve this by allowing state exceptions and complex rules regarding when those exceptions apply. Furthermore, a well resourced nationally consistent process for managing privacy complaints (i.e. not delegated to state/territory as proposed in 56-1) would be more appropriate considering today's ubiquitous technology.

2) **Capabilities of Human Research Ethics Committee (HREC)**

Greater reliance on referral to the Human Research Ethics Committees (HREC) is being proposed for interpreting a wide range of health data study and analysis. This includes interpretation of the boundaries between research and quality assurance/audit (addressed in key point 8 below). We continue to recognise that the HREC play a valuable role as the protector of health data for research purposes. Concern has been raised that currently there is not sufficient consistency across the various HRECs and many do they have the necessary skills and resources to carry out the proposed functions as proposed by the ALRC discussion paper. In particular, concern has been raised about how to avoid the inevitable bureaucratic backlog associated with HRECs unless these issues are adequately addressed.

3) **Wider Stakeholder Involvement**

There is a proposal to develop guidelines that relate to the "handling of health information under the Privacy Act" (56-4). The stakeholders involved will be at the discretion of the Office of the Privacy Commissioner with only DoHA being specifically mentioned. The range and types of stakeholders need to be specified to ensure adequate industry and professional society representation.

4) **Maintaining Technology Neutrality**

Technology changes rapidly and hence any 'technology neutral' proposal must therefore rely on the basic principals (UPPs) set down in the Act. Are sufficient provisions being made to accommodate how inevitable changes in technology will need to be interpreted as being compliant with the UPPs in the Act? International evidence has shown that too much damage will be done to consumer trust if we have to wait for case law. Hence, the necessity to incorporate regular periodic risk assessments of new technologies and interpretive guidelines would greatly assist in maintaining people's confidence with technology. Furthermore, concern over the proposal to establish specific 'enabling' legislation for Unique Health Identifiers (UHI) and Shared Electronic Health Records (SEHR) is considered to be at odds with technology neutrality and the move towards 'consumer directed healthcare' (addressed in key point 5 below).

5) Towards 'User-Centric' Health Provision

In health we have witnessed changes in people's (clients) expectations and behaviour brought about by the advances in technology. That is their ability to access health knowledge and to take greater personal control over their health to include user controlled internet content (e.g. Web 2.0). Furthermore, personal access to medical devices, assistive technologies and the future 'smart home' environments are causing a shift towards data being held by non traditional healthcare providers. Although the proposed privacy law changes intend to be 'technology-neutral' they need to recognize this shift in behaviour brought about by technology. Evidence of how individuals are violating the privacy of their family and colleagues is provided in the commentary section below to emphasise the undesirable consequences of users with access to the internet. Current proposals focus on 'health service' and 'health service providers' and not the responsibility of individuals.

6) Pragmatic Approaches to Consent Issues

Consent is a complex yet absolutely crucial component in the continued move towards computerized health data. Evidence shows that it is an area where we rarely see any consistency even at the state level. For example, in some states every hospital's consent form is different with high levels of uncertainty over its legal standing. Getting the right balance between the need to gather health data for analysis for the common good and the right to individual's privacy may ultimately depend on interpretations of 'reasonableness' in obtaining consent. To achieve national guidelines that are both pragmatic and widely acceptable will require much greater investment and resources in privacy management and education than currently proposed.

7) Recognition of National and Globalisation trends with Health Data

Common platforms for the application of privacy need to take into account the increase in cross border data flows. Many of our industry partners are requesting a 'global' approach to ensure a baseline standard across the industry and organizations. It is not uncommon for industry to make use of international partners to provide business continuity by ensuring backup and hot-standby operation is available. Reliable access to health data on demand needs such resilience. Reforms could include the establishment of a national body to provide guidance to ensure potential partners both nationally and internationally are sufficiently compliant with our standards.

8) Support for Clinical Audit and Quality Assurance

Concern has been raised over a lack of support from the proposed Privacy legislation and Health Information regulations to facilitate Clinical Audit (CA) and Quality Assurance (QA) processes for continuous quality improvement of clinical services. The ALRC proposal is to regulate this through the exception rules 57.205-230. The reliance on management activity rules issued by the Privacy Commissioner (57.225) may be compounded by some activities being characterised as research (57.227) resulting in increased workload for HREC and data custodians with a risk of serious delays and non-compliance. Some possible solutions to help alleviate this are provided in the commentary section below.

Background

HISA (the Health Informatics Society of Australia) welcomes the opportunity to provide this submission to the Australian Law Reform Commission.

Health Informatics deals with the resources, devices and methods required to optimize the acquisition, storage, retrieval and use of information and knowledge in health and biomedicine. HISA provides a national focus for this discipline, its practitioners, industry and users.

With over 400 members, HISA represents a broad range of health practitioners (physicians, nurses and allied health care providers), IT specialists, health care management, technology suppliers and academics. As such, HISA is uniquely positioned to understand and provide comment on the issues surrounding information privacy in the health arena. HISA is in active discussion with its member base through a regular process of survey, evaluation and discussion. One of our core objectives is to stimulate the insightful analysis of the issues surrounding health information. Any Privacy legislation is key to HISA members, the majority of whom are directly responsible for handling sensitive health data in their capacity as data custodians, clinicians, health managers / administrators and health researchers. We encourage the Australian Law Reform Commission to take further advantage of HISA as a reference resource, as it continues in the development of its privacy submissions.

What has HISA done in Health Privacy and Security?

Since the release of the ALRC's issue paper 31, consultation of our members plus the wider health informatics community has been instigated through a number of avenues.

This included a national symposium in October 2006 on Privacy and Security of electronic health (ehPASS'06) where Carolyn Adams from the ALRC was invited as a special presenter following the release of the issue paper. At this event, attended by 60 delegates from across 5 states/territories, Professor Peter Croll (chair of ehPASS'06) announced that HISA would be making a submission on behalf of the HISA members and wider community to the ALRC. To facilitate this, a national survey was conducted with HISA members and associate health organisations specifically focussed on the health sections of issue paper 31 (chapter 11).

The HISA board agreed in Nov 2006 to form a special interest group focusing on Privacy and Security issues known as HIPS with a committee formed from national experts in the area.

A further ehPASS workshop was conducted at the International Medinfo 2007 conference in August with representation from key international players specialising in health privacy.

In September 2007, HISA initiated a national survey across both its members and across members of the consortium of professional society relating to health. One

section was dedicated to Privacy and Security of Health information. These items were ranked as of the highest importance from the respondents and the detailed comments have been included in this submission.

In November 2007, the HIPS group organised a national forum hosted by Microsoft in Sydney at which key national presenters were invited to include Professor Michael Frommer who is leading the NCRIS initiative to establish the national data linkage centre for population health studies. Members who attended this event were consulted on this submission at this event and invited to comment via the HIPS web forum pages (www.hisa.org.au/hips) set up for this purpose.

Any changes on HISA's previous position?

In our previous submission to the ALRC we highlighted three key areas of concern. These included national consistency, obtaining individual's consent and the need to address the risks associated with evolving technologies, as follows:

"Overall our members are seeking national consistency in future privacy regulations. Exclusions for state and private sector only add unnecessary complexities that instil mistrust in the sharing of data. The National Health Privacy Code has not been an effective vehicle to achieve this to date and practitioners simply don't know where they stand legally on many key issues. Separate privacy principals for Health would also permit definitions associated with current working practices and help clarify the interpretation of key issues. Consent is seen as a critical area where there is a need to clarify the legal standing for collection and access to health data not only for the health practitioner's understanding but to ensure future technology can be built robustly to comply. The risks associated with new technologies is a continuously moving target and the future regulations should recognise this by requiring a provision for ongoing assessments and preventative actions that minimise and risks of privacy and security violations with health information management."

Fundamentally our position has not changed. The eight key points now identified in this submission above now include more comment arising from interpretation of the ALRC's discussion papers and proposals. Further insight from where technology is heading has provided additional points, for example the user-centric view on health data and the globalisation issues.

The following are the original proposals in our earlier submission. We note and welcome the fact that many of these points have been addressed in the ALRC's discussion paper 71. The following commentary section highlights some of the concerns that, if appropriately addressed, would in our opinion greatly benefit the interpretation and implementation issues associated with the pragmatics of privacy protection of health data.

Original points raised in HISA's submission to the ALRC (Jan 2007):

- i. With regard to health information all agencies and organisation should have to comply with future privacy acts.*
- ii. Future privacy acts should make provisions to exclude any health data that has been suitably de-identified.*
- iii. Consent should be sought from interested third parties before they introduce any scanning technologies that can lift personal health and medical information.*

- iv. *Definitions of what constitutes sensitive data should be brought up to date so that biometric, genetic and other related identifiable health related information is included.*
- v. *Special provision should be made in future legislation to deal expressively with the situation in which a health service provider ceases to operate to ensure ongoing, timely and appropriate access to health data.*
- vi. *Future privacy acts address appropriately the consent issues associated with the collection of and access of an individual's health data.*
- vii. *Clear guidelines on the circumstances and safeguards necessary for overriding any standard consent requirements should be included for the circumstances where an individual has limited capacity to provide such consent.*
- viii. *First and foremost the individual should feel that their health data is adequately protected over the public interest in promoting research.*
- ix. *In clarifying and strengthening the consent legislation then provision for consenting to insurance companies should be included.*
- x. *Any future legislation should clarify the situation of when the federal act applies and try as far as possible to avoid grey areas associated with interpretation of inconsistencies between federal and state acts.*
- xi. *Care should be taken to ensure that any rights given to individuals to access personal data should include specific allowances that protect therapeutic relationships with a health care service provider that is in the interest of a patients well being.*
- xii. *Special provisions should be include in any future acts to deal specifically with health data privacy principals that would include definitions of terms associated with common practice, e.g. clinical audit, quality assurance, health research and differentiation between health service and health information.*
- xiii. *Human Research Ethics Committees should remain as a key protector of health data for research purposes yet future legislation should provide clearer guidelines over consent and health research definitions.*
- xiv. *Future privacy acts can not be technology neutral and should take into account the fragility and vulnerabilities associated with commodity software to ensure that ongoing privacy and security risk assessments are incorporated whenever computer technology is employed for managing health data*

Commentary

The following commentary provides additional detail to the eight key points outlined in the Key Point/Executive Summary section above. This commentary was collected through the online discussion centred around the output of the November Privacy Seminar. There were also a number of direct submissions for participants in the seminar.

1) National Consistency

The majority of HISA members seek national consistency with the proposed privacy laws across both the State/Federal and Public/Private sectors. The current proposals do not go far enough to resolve this by allowing state exceptions and complex rules regarding when those exceptions apply. Furthermore, a well resourced nationally consistent process for managing privacy complaints (i.e. not delegated to state/territory as proposed in 56-1) would be more appropriate considering today's ubiquitous technology.

Comment 1:

“The ALRC must acknowledge the progress of the Council of Australian Governments (CoAG) and its proposed establishment of a national registration and accreditation scheme for health professionals. Any proposed regulatory framework for health informatics must, therefore, integrate with the new national scheme. Not all state/territory has a health services commissioner or some other independent person to oversee complaints against health practitioners (esp those not subject to statutory registration). In addition, not all health services commissioners oversee complaints in relation to breaches in relation to privacy. There is a “patchwork” of regulatory bodies (who can apply penalties and sanctions), independent health commissioners (who often provide remediation and dispute resolution services) and sometimes privacy commissioners. Assuming the ALRC is across all these issues, there needs to be clear guidelines of where their powers start and finish so that consumers are in an informed position to raise issues as they encounter them. If the ALRC suggests some form of Commonwealth legislation to create a new independent statutory body to regulate health information, it must consider not only national implications but also international implications as “e-health” info can be readily shared over the internet.”

Comment 2:

“I would prefer to see all potential uses of health information, including sharing of information between healthcare providers for the purpose of providing health care services, covered by uniform legislation and regulation. As discussed at the HISA Privacy Seminar, it can be difficult to discern secondary use of data for quality assurance from use for research, for example. The lines are seldom clear or well defined. A uniform approach to consent, sharing, and access for secondary use supported by a well resourced national authority for health care information would allow people

"at the coalface" to negotiate solutions suitable for the requirements thrown up by their particular situations. 57-1 The definition of 'health information' in the Privacy Act should be amended to make express reference to information or an opinion about the physical, mental or psychological health or disability of an individual. This seems a sensible amendment to suggest. I think the definition of a monolithic SEHR embodied in legislation as suggested above would be difficult under such a broad definition."

2) Capabilities of Human Research Ethics Committee (HREC)

Greater reliance on referral to the Human Research Ethics Committees (HREC) is being proposed for interpreting a wide range of health data study and analysis. This includes interpretation of the boundaries between research and quality assurance/audit (addressed in key point 8 below). We continue to recognise that the HREC play a valuable role as the protector of health data for research purposes. Concern has been raised that currently there is not sufficient consistency across the various HRECs and many do they have the necessary skills and resources to carry out the proposed functions as proposed by the ALRC discussion paper. In particular, concern has been raised about how to avoid the inevitable bureaucratic backlog associated with HRECs unless these issues are adequately addressed?

Comment 1:

"HRECs have been around for many years and there is considerable concern about the mode of interaction between lay advisers, clinical professionals and non clinical professionals. Expertise of a high level is vital if 'group think' and power dynamics are not to distort outcomes and adequately protect patients and subjects. Adequate and skilled resources are crucial as researchers livelihoods depend on efficient and reliable responses."

Comment 2:

"Defining what "health" is can be problematic. Many clinicians are moving towards "consultancy" services (eg. Job placement agencies for the disabled, organisational psychology, OH& S etc). One doubts if the HREC has the broad representation, expertise and resources as well as the ability to draw expertise and input from a variety of sources in order to make timely and informed decisions."

Comment 3:

"With all due respect for their abilities, I don't think that Human Research Ethics Committees are the right bodies to take a prominent role in such a broad based process of change, although they are clearly valuable resources. Devolution of complaints management to the individual State jurisdictions runs the risk of dissipating responsibility and would make it harder to provide effective leadership. I would prefer to see a more integrated approach to the operational and practical issues in finding and maintaining the right balance. Such an approach would (I think) have to be a single national body, and would either take advice from or subsume the functions of the various Committees and Commissioners that currently exist."

I cannot describe the exact nature of the body I think should be responsible for this, but I'm sure there are experienced people out there who can make some very practical and positive suggestions along these lines."

Comment 4:

"Regarding ALRC Proposal 58–3: The Privacy Act should be amended to provide that 'research' is any activity, including the compilation or analysis of statistics, subject to review by a Human Research Ethics Committee under the National Statement on Ethical Conduct in Human Research (2007).

- *This provides a strong platform for the requirement of all QA activities to be characterized as research on the basis of the National Statement guidance, which will require separate HREC submission and approval*
- *'sample acquisition' -identification of a population with specific characteristics relevant to a study proposal prior to undertaking a study to determine feasibility for development of a study proposal would also require HREC review, (58.218). This is a frequent activity in relation to QA practices.*
- *A submission by NHMRC urged the 'ALRC reconsider the role of HRECs in decisions about the privacy implications of the collection, use or disclosure of health information in research. The NHMRC is of the view that these considerations could be managed without intervention by an HREC although we have not identified a replacement mechanism at this stage' (58.120)*
- *Despite this suggestion, the ALRC continues to recommend HREC review of all health information study proposals, albeit with guidance by rules developed by the Privacy Commissioner:*
- *Proposal 58–12: The Privacy Commissioner should address the following matters in the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle:*
 - *the process by which a Human Research Ethics Committee should review a proposal to examine a health information database or register to identify potential participants in research; and*
 - *the matters a Human Research Ethics Committee should take into account in considering whether the public interest in allowing the examination of the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the proposed UPPs.*
- *This proposal again indicates a requirement for the HREC review of disclosures from a health information database"*

3) Wider Stakeholder Involvement

There is a proposal to develop guidelines that relate to the "handling of health information under the Privacy Act" (56-4). The stakeholders involved will be at the discretion of the Office of the Privacy Commissioner with only DoHA being specifically mentioned. The range and types of stakeholders need to be specified to ensure adequate industry and professional society representation.

Comment 1:

“Obviously there needs to be full stakeholder consultation and consensus building with item 5 and there must be appropriate protections with cross border flows of sensitive information (I suggest must have as good a regime or better before data moves OS).”

Comment 2:

“National guidelines on obtaining individual's consent are crucial. This would permit unified approach to recording client's preferences and ensure technological compatibility for sharing and linking health information. Also need to consider clients that are receiving treatment against their will (sectioned patients in acute psychiatric facilities). Again, only the most privileged of clinicians should have access to this record and having their access logged. Patients should have the right to view or access those “sectioned” records once they recover.

Any reform in e-health must be integrated with other health reforms. Health is undergoing rapid transformation. There is a trend towards “nationalisation” of services which removes duplication and costs to consumers. However, the downside of such move is the trends towards “lowest common denominators”, which, in turn hampers the development of “best practice” models.

There are agreements to establish a national registration and accreditation scheme for health practitioners. There are also plans developed to reform the private health insurance market to allow insurance providers to offer “hospital substitution services” outside of hospitals such as home dialysis and chemotherapy. In addition, the Australian Commission on Safety and Quality in Health Care is reviewing the national accreditation standards for health services and has released a series of discussion papers for industry consultation and feedback. The ALRC must be cognisant of these developments and their possible impact on the ALRC proposals.”

Comment 3:

“There is no substitute for well informed people when seeking judgement and balance. Achieving and maintaining the right balance between public good, practicality and individual preferences will require ongoing effort from people committed to the task. At the same time, I think there is a growing recognition that for health information, the current balance is not right, that there is a need for change. In exploring this, we should consider a broad range of topics such as the notion of ownership of information, practical limitations on personal control of information, currently available technical solutions and their limitations, changing expectations of consumers, transition issues, and so on. Some of these issues will be best dealt with through provisions in the legislation, others will be better managed through regulation and governance. The situation is crying out for an individual or small committee with a mandate to lead the consultations and once a solid consensus has been established, push through the required changes. The entire process needs to be very well resourced, starting with significant and wide ranging stakeholder consultation. Following this, there will be a need to

support people (both health care providers and consumers) through the required changes in practice that will (I believe) emerge from the consultations.”

4) Maintaining Technology Neutrality

Technology changes rapidly and hence any ‘technology neutral’ proposal must therefore rely on the basic principals (UPPs) set down in the Act. Are sufficient provisions being made to accommodate how inevitable changes in technology will need to be interpreted as being compliant with the UPPs in the Act? International evidence has shown that too much damage will be done to consumer trust if we have to wait for case law. Hence, the necessity to incorporate regular periodic risk assessments of new technologies and interpretive guidelines would greatly assist in maintaining people's confidence with technology. Furthermore, concern over the proposal to establish specific ‘enabling’ legislation for Unique Health Identifiers (UHI) and Shared Electronic Health Records (SEHR) is considered to be at odds with technology neutrality and the move towards ‘consumer directed healthcare’ (addressed in key point 5 below).

Comment 1:

“There needs to be a careful distinction drawn between privacy principles - which must be technologically agnostic - and just serve the need for privacy - and the implementation of privacy - be it in paper, technical or organisations and their systems. Each implementation has different issues to be addressed to ensure the principles are met.

People need to be confident that no matter what technology is in play at any given time their personal health information will be protected from misuse and abuse. To be technology neutral this legislation needs only to focus on the right of the individual to have their privacy protected by law rather than trying to cover all possible circumstances with separate clauses. I'd like to see fewer exceptions and exemptions and much more consistency. I'd also like to see some consideration of penalties when breaches do occur.”

Comment 2:

“I could not agree more with the comments above regarding consent and consensus building. While in an ideal world, the legislation should be “implementation neutral”, we ignore practical implementation issues at our peril. Avoiding the problem by leaving the resolution of some of the more pressing practical issues to case law is likely to lead to further uncertainty and delay. I agree that once we move beyond the straightforward cases, there is often no “right” answer, and the legislation and regulatory framework should recognise this from the outset.

** 56-5The national Unique Healthcare Identifiers (UHIs) scheme and the national Shared Electronic Health Records (SEHR) scheme should be established under specific enabling legislation. The legislation should address information privacy issues, such as:the nomination of an agency or*

organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;

- A. the eligibility criteria, rights and requirements for participation in the UHI scheme and the SEHR scheme by health consumers and health service providers, including consent requirements;
- B. permitted and prohibited uses and linkages of the personal information held in the systems;
- C. permitted and prohibited uses of UHIs and sanctions in relation to misuse; and
- D. safeguards in relation to the use of UHIs; for example, that it is not necessary to use a UHI in order to access health services.

Some of the above looks strangely familiar - like a single national body with responsibility for managing a single, monolithic "Shared Electronic Health Record" - something that we are apparently no closer to despite significant efforts over many years. If the UHI is created and used, I think it is much more likely that sharing of health information will take place on a smaller scale. The effect of this would be to create many "SEHRs" in a dynamic fashion, focused around the needs of individual consumers. This approach would be more in line with the growing "consumer directed healthcare" movement. In fact, having specific legislation covering one particular technology - centralised data collection forming a shared electronic health record - seems to be at odds with the principle of being technology neutral."

5) Towards 'User-Centric' Health Provision

In health we have witnessed changes in people's (clients) expectations and behaviour brought about by the advances in technology. That is their ability to access health knowledge and to take greater personal control over their health to include user controlled internet content (e.g. Web 2.0). Furthermore, personal access to medical devices, assistive technologies and the future 'smart home' environments are causing a shift towards data being held by non traditional healthcare providers. Although the proposed privacy law changes intend to be 'technology-neutral' they need to recognize this shift in behaviour brought about by technology. Evidence of how individuals are violating the privacy of their family and colleagues is provided in the commentary section below to emphasise the undesirable consequences of users with access to the internet. Current proposals focus on 'health service' and 'health service providers' and not the responsibility of individuals.

Comment 1:

"Need to define what "health services" are (or stating what they are or should not be), see point above. The right of consumers not to disclose certain information must be respected, esp in sensitive areas such as mental health. However, this challenges the integrity of the data collected and how they may be interpreted and used for epidemiological studies (ie. Underreporting of depression does not mean depression is on the decrease).

The need to define what constitutes “health” records: Health services are no longer seen as “hospital and like” services. They are increasingly expanding into alternative, preventative and consultative services such as Chinese medicine, yoga and life coaching but to name a few. Even within traditional health services, mental health services often warranted its own special place and often with very valid reasons. Governments at both Commonwealth and state/territory levels have developed specific regulations in dealing with health records, with some specifically outlining how mental health records must be kept separate from “general” health information and only accessible to those on a “need to know” basis, the NSW Privacy and Personal Information Protection Act (1998) is one such act. It might be useful for the ALRC to outline what it considers to be “health” records (or define what they are not) to put any proposals it recommends into context for readers.”

Example of internet users publicising relatives health problems: The following are two recent examples where individuals have taken to using the internet to gain help with medical related issues. They both emphasise the fact that it would not be ‘unreasonable’ to identify the relatives involved where their health problems have been revealed. These are only excerpts with other postings giving more details such as job function/school location etc. of the individuals being talked about. They are provided as examples where health information is being made available, without any obvious consent, on public forums and once posted can not be readily removed and is likely to remain for years to come. (Note: for both of the following cases, and before adding to this submission, the names, places and ages have been modified to de-identify the original senders).

Catherine (Adelaide) wrote:

Hi guys,

I am really struggling here and need some sane advice, I think.

My Husband is bipolar, diagnosed for 25 years, but is currently having his first episode in twelve years. So whilst it's definitely not his first episode, it's mine, if you know what I mean. an hour later he was wrestled to the ground by police after threatening to kill me and the babysitter I had hired to watch the kids so I could try (for a FOURTH time) to take him to hospital. This was on the 9th December. My birthday is the 10th..... My dear daughter (aged 7) told me her grandmother wanted to know if she could still come for Xmas. Dad left msg saying they could maybe take kids, but maybe dear husband needed them around as part of his therapy. He told me I should resign my job because they obviously aren't worth working for. Now, this is my dream job that we as a family have been working towards and I have been studying for 5 years. Dad didn't believe that I had to go back to work because everyone knows Unis have a break over Summer. He apparently doesn't know that this is the third year in a row I've taught Summer session.

I am ready to cut off my parents altogether over their handling of all of this, but I also know I am overly emotional at the moment. What I do know is that my friends are rallying and I've seen neither hide nor hair of my parents, who only live 3 hours away. My mother-in-law in contrast got on a plane as soon as she heard and flew here from VIC for the first five days. My brother-in-law and his partner are on their way here in their camper bus thingy -- instead of going to Woodford, as planned.....

Rebecca (Perth) wrote:

Tom, I read that site you posted. I'm in the middle of picking up my jaw off the ground. Part of it were like reading about my daughter's twin. My Brother also has 4 girls, aged 12, 10, 5 & 2. The 12 year old has ADAH and is treated with Dexamphetamine and the 5 year old has Asperser's - too young for medicine yet. My brother-in-law has a 13 year old with ADD and she uses Ritalin. Her son isn't hyperactive, just learning difficulties. I am very concerned about the long term effectsI also have a dear friend with 2 children aged 10 and 8. The eldest has always but was never diagnosed, the 8 year old has ASD and....

6) Pragmatic Approaches to Consent Issues

Consent is a complex yet absolutely crucial component in the continued move towards computerized health data. Evidence shows that it is an area where we rarely see any consistency even at the state level. For example, in some states every hospital's consent form is different with high levels of uncertainty over its legal standing. Getting the right balance between the need to gather health data for analysis for the common good and the right to individual's privacy may ultimately depend on interpretations of 'reasonableness' in obtaining consent. To achieve national guidelines that are both pragmatic and widely acceptable will require much greater investment and resources in privacy management and education than currently proposed.

Comment 1:

"The suggestions made do not to my mind come near addressing the complexity of how consent should be obtained, managed, refreshed and how the legion of different types of primary, secondary and even tertiary information should be treated. As soon as you move from the individual rational and competent individual freely giving informed consent for a specific act or treatment you move into areas where judgment and balance are required - e.g. all secondary data use etc etc. The differential sensitivity of varieties of health information adds an additional layer of complexity that needs consideration as well.

The sections dealing with exceptions in regard to reporting and research are of concern to me. The use of the criteria of impracticality as a trigger to allow the use and disclosure of health information without consent seems exceptionally vague. What is the test of impracticality? It seems to me that it will always be "impracticable" to contact a multitude of individuals to seek their consent each time someone wants to gather data. And this is just one of the criteria listed that allow disclosure without consent. The clauses seem to apply to all data including identifying data where it is deemed to be necessary to use it. Overall the changes appear to further weaken the

control of the individual over their personal health information. The individual's right to privacy is sidelined in preference for centralized control and expedient managerial decision making. I agree with previous comments that the mechanism for attaining consent should be addressed.

Where there is otherwise a requirement for consent for a particular activity involving health information in the context of reporting/research, the waiving of the need for consent due to the criteria of impracticality should be evaluated by an authority such as an HREC or alternative approved review mechanism. The issue of consent is discussed in Chapter 16 of the ALRC review and in paras 58.90-106. OPC guidelines on the subject state: 'impracticality' should be something more than incurring some expense or effort in seeking an individual's consent" and provides the following examples:

- *individuals may be uncontactable due to death or relocation (this particularly arises in relation to old records);*
- *individuals of interest may be part of a demographic group that is difficult to contact (for example, remote/indigenous groups);*
- *the number of records involved may cause logistical problems; or*
- *the objective of the investigation may need to be concealed from subjects in order to minimize various forms of bias. For example, having to obtain consent in blind trials could compromise the integrity of the research. (58.101). The impracticability exception is clearly not intended to be a standalone rule, but is 'one of the criteria an HREC or other review body must consider in determining whether to grant waiver of consent...' (58.104). Consent should not be used gratuitously for its own sake. Rather it should be considered one of the tools (albeit one of the most significant) available to ensure due respect and consideration is afforded individuals in the handling of their information. Certain aspects of information use are integral to clinical service provision, both the patients current service and in being able to provide the service in an ongoing manner. Inappropriate use of consent can lead to confusion in the public eg different practices in requesting consent for the purpose of transferring information to other professionals involved in the ongoing health service provision of the individual. This also creates an unnecessary burden on the individual and further useless documentation. The instances where consent for information use is not required should be carefully defined and regulated by an appropriate body with identifiable delegation at the service level. It should be clear to patients how their information is used and protected (and their avenue for individual special protection) and how this then contributes to achieving the expectation of the quality services demanded. Appropriate use of information goes beyond obtaining consent. An essential element not well addressed is education of both the public and health professionals in this area. This requires the provision of resources (both financial and*

directional) to support Privacy management of health information (beyond HRECs provisions for research) in a quality manner.”

Comment 2:

“The “law of averages” is a good test in any new proposal. The tension in the ALRC proposal is getting the balance right between the need to gather, interrogate and disseminate data and the right to privacy by consumers. There is a need to set some objective boundaries around “reasonable-ness” as well as rule for “exceptional circumstances”, esp in relation to research activities and data linkages for population health studies. However, as stated from the outset, the right of individuals must be paramount and overrides the need for data integrity.

Privacy and informed consent:

The notion of “informed consent” need to be further elaborated. The health service providers were granted privileges to access a person’s health records via an informed consent. They must not abuse that privilege by releasing those records without additional explicit consent from the consumer (eps in relation to sensitive information), or fail to protect the unauthorised access to those records using appropriate measures such as encryption. A person’s health record must only be viewed by those who has been given consent to view it AND those who must view it (ie. On a need to know basis). The individual must have the right to review and revoke providers’ privileges in accessing, viewing and transmitting their health records, as well as the right not to disclose information to providers.

The non-traditional health sector (such as insurance agents) should develop and adhere to a set of E-Health and Privacy Services Guide, similar to those used by financial institutions, to explain to its customers how they collect, transmit and secure their health records. Moreover, the guide should explain to consumers their rights and privileges and avenues for complaints.

The issue of “involuntary consent”, such as those in “sectioned” acute mental health facilities warrants further clarification. The APS is of the view that once a person recovers from their acute episode, that they will have full ownership of any health records collected during their sectioned period, and therefore can decide who and how such records can be accessed and transmitted.

The rights of individuals must be paramount

Health records are specific to individuals, who must have full ownership to them unless in exceptional circumstances such as during an acute mental health episode. The right of individuals must prevail over any need to collect, interrogate and report data, especially if that data is sensitive or can be readily attributed to individuals.

In considering privacy and e-health, the most important questions should be:

- *Who is collecting the health data*
- *For what purpose*
- *How it might be used by others who have access to the data*

- *What safe guards are in place to de-identify data and to protect them from un-authorized use?*
- *What safe guards are in place for data storage, retrieval and transmission to minimise loss, unintentional release or un-authorized access?*
- *Therefore having different levels of access are important to maintain the rights of individuals (eg. The hospital porter does not have access data only privileged to the surgeon etc)."*

7) Recognition of National and Globalisation trends with Health Data

Common platforms for the application of privacy need to take into account the increase in cross border data flows. Many of our industry partners are requesting a 'global' approach to ensure a baseline standard across the industry and organizations. It is not uncommon for industry to make use of international partners to provide business continuity by ensuring backup and hot-standby operation is available. Reliable access to health data on demand needs such resilience. Reforms could include the establishment of a national body to provide guidance to ensure potential partners both nationally and internationally are sufficiently compliant with our standards.

Comment 1:

"The concept of a single national body to provide direction and regulation for health information seems valuable. The NHMRC represents a very successful model of regulating Australia's health and medical research practices to provide a platform of exemplary global standard. However Health information has much broader application than the research bias of the NHMRC may be able to support and the NHMRC has itself implied as much. Expertise and practical guidance on the use of health information from organisations such as the AIHW as well as DoHA are required. Ultimately, a national body would then be able to provide guiding documentation to which legislation could refer (eg similarly to the NHMRC National Statement), providing some greater flexibility for response to unforeseen changes than the legislative review process. This body could also have a supporting role for ongoing professional education processes for Privacy and information use, in which Australia may lag behind nations such as the US and UK. It is important however, that this does not simply become another layer of regulation, and that States must comply with this single regulatory process, much as for the NHMRC regulation of human research nationally."

8) Support for Clinical Audit and Quality Assurance

Concern has been raised over a lack of support from the proposed Privacy legislation and Health Information regulations to facilitate Clinical Audit (CA) and Quality Assurance (QA) processes for continuous quality improvement of clinical services. The ALRC proposal is to regulate this through the exception rules 57.205-230. The reliance on management activity rules issued by the Privacy Commissioner (57.225) may be compounded by some activities being characterised as research (57.227) resulting in increased workload for HREC and data custodians with a risk of serious delays and non-compliance. Some possible solutions to help alleviate this are provided in the commentary below.

Comment 1:

Clinical Audit/Quality Assurance is regulated by the exception rule in the Proposed Privacy (Health Information) Regulations: Management, Funding or Monitoring of a health service under IPPs (57.205-230)

- *In the context of CA/QA this relates to disclosure and use of non-consented identifiable information collected for the primary purpose of the health service (ie medical record) with possible collection into a register or database and further disclosure and use again.*
- *“The NHMRC has noted that some management activity does not amount to research and does not require review by an HREC.196 In the ALRC’s view, in these circumstances the activity should be able to proceed simply on the basis of rules issued by the Privacy Commissioner“ (57.225) HOWEVER*
- *“57.227 The ALRC notes that some funding, management, planning, monitoring, improvement and evaluation of health service activities also may be characterized as research. Where particular activities can be characterized as both management activities and research the ALRC is of the view that the activity should be conducted in accordance with the proposed rules issued by the Privacy Commissioner and should also be subject to the provisions relating to research, discussed in the following chapter. The proposed research provisions, like the s 95 and s 95A guidelines, provide for review of research proposals by an HREC.”*
- *Characterization as research requires HREC review*
- *Definition of Research is difficult*
 - *National Statement on Ethical Conduct in Research Involving Humans —June 1999*
 - *There are many definitions of research. These include systematic investigation to establish facts, principles or knowledge and a study of some matter with the objective of obtaining or confirming knowledge.*

An alternative approach to finding a definition of research is to list examples of what constitutes research, such as:

- *systematic prospective collection of information to test an hypothesis;*
- *a planned study of existing practices with a view to changing/improving practice in light of the study's findings and/or to increase understanding; or*

National Statement on Ethical Conduct in Human Research (2007)

Human research is conducted with or about people, or their data or tissue. Human participation in research is therefore to be understood broadly, to include the involvement of human beings through:

- *taking part in surveys, interviews or focus groups;*
- *undergoing psychological, physiological or medical testing or treatment;*
- *being observed by researchers;*
- *researchers having access to their personal documents or other materials;*
- *the collection and use of their body organs, tissues or fluids (eg skin, blood, urine, saliva, hair, bones, tumour and other biopsy specimens) or their exhaled breath;*
- *access to their information (in individually identifiable, re-identifiable or non-identifiable form) as part of an existing published or unpublished source or database.*
- *Many or most QA processes can therefore be characterized as research according to the National Statement*
- *National Statement advises any human research of greater than 'low level of risk' requires HREC review:*
 - *definition of 'low risk' re handling of sensitive information: ALRC is of the view that disclosure of non-consented sensitive information for a purpose that is not directly related to the purpose of collection and within the reasonable expectations of the individual "is likely to involve more than a low level of risk for individuals and should always be reviewed by an HREC". (58.129)*
 - *definition of 'directly related purpose' does not include management, funding, monitoring' which is handled by a separate exception rule. 'Directly related' refers to activities relating directly to the clinical service provision of the individual concerned, therefore QA activities cannot be excepted by virtue of being directly related*
- *The National Statement refers to the NHMRC advisory document "When does Quality Assurance in health care require independent ethical review" which*
 - *facilitation of QA activities*
 - *indicates distinction of Clinical Audit and Quality Assurance studies as separate from research studies, which are seen to be lying on a continuum, is difficult*
 - *interprets National Statement constraints more permissibly for the purpose of QA*

- suggests simpler mechanism for authorizing QA activities (but still requiring QA proposal submission to HREC or delegate)
- not as well known/distributed document as National Statement

Potential of Electronic Health Data in Clinical Service Improvement

- *At a plenary session of MedInfo07, 12th World Congress on Health (Medical) Informatics (Brisbane 20-24 August), it was noted that data acquisition automation and connectivity quadrants of eHealthcare systems are well developed, however currently eHRs lack maturity in the decision support and analysis quadrants, eg data mining, ad hoc analysis, however this is now in a rapidly developing phase.*
- *This analysis area has the greatest potential for supporting continuous quality improvement into the future eg*
 - *Automated assistance with technical aspects of care*
 - *Grouping treatment and outcome data from previous rare patient subsets to provide real time guidance for a similar inpatient in the context of the individual healthcare institution*
 - *Development of new outcome measure*
 - *Examine large amounts of data for meaningful patterns*
 - *Facilitate data collection and case-mix adjustment for TQM purposes*
 - *Many unforeseeable analysis developments and strategies*
- *Note again that many analyses based on the compilation or analysis of statistics from health information can be carried out on anonymised records, however the information is derived (=disclosed) from necessarily identifiable records and must be re-identifiable for the purpose of possible closer examination of specific documentation in some circumstances, retaining the element of 'greater than low risk'*

Risks for Health Services of overprotective Privacy regulation

The NHMRC states (57.42): There is, in fact, considerable potential for individual harm as a result of a privacy regime which results in individual health care providers being uncertain about their legal obligations, afraid of breaking the law by transferring health information without explicit consent, and implementing ineffective and inefficient procedures in their efforts to comply with the law.47

This was made in reference to the poor transfer of health information between providers resulting in harm to an individual; however the statement can extend to the processes of Clinical Audit and Quality Assurance, where poor facilitation can cause considerable harm to continuous improvement of the clinical service.

Risks: Over-compliance/Non-compliance

- *Implications for interpretation of policy makers re electronic health information collection/disclosure and use policies- policies developed primarily by Information Directorate staff, which have limited clinical background*
 - *Limited understanding of the practical clinical requirements for use of health information can lead to impractical interpretation and policy development*
- *Implications for HRECs*
 - *Question of adequacy of knowledge re eHR for determining appropriate balance of public interest in benefit vs privacy – frequent bias towards overprotection of individuals privacy rights*
 - *Extra burden – extra submissions, 6 monthly report documentation, questionable timeliness of approval response*
- *Implications for clinical service*
 - *QA activities more difficult, requiring HREC proposal development and submission, multiple signatures*
 - *Delays*
 - *Risk of Non-compliance*
- *Implications for database custodians/data managers*
 - *Could be compromised where requests might be made without full HREC approval*
 - *Increased workload managing submission process*

Possible Solutions:

- *There must be protection against frivolous use, inappropriate information access and poor analysis and study methodology, so there must be appropriate authority sought, but it must be a quick process with a clinical basis not inhibited by the logistics of convening of a committee.*
- *NHMRC suggested an alternative to HREC review for use of health information in medical research, but was not able to suggest a mechanism – some suggestions are made in the “When does Quality Assurance in health care require independent ethical review” advice paper.*
- *Recommendations from NHMRC advisory document “When does Quality Assurance in health care require independent ethical review” needs to be better reflected in the Privacy (Health Information) Regulations*
 - *Legislation could explicitly exclude QA along with Clinical Audit/performance monitoring based on clear purpose definition of the intension of local service improvement together with details of protective structures for rapid authority and approval separate from HREC review*
 - *Legislation could allow a single HREC submission to cover current and future QA activities by the service obtaining approval to use and disclose the information for the purposes of Clinical Audit and QA activities only as authorized by a medical HOD (who is bound by a professional code of conduct) and provided that the HREC is satisfied with the protective measures and policies developed by the unit/service to ensure confidentiality is maintained during subsequent*

QA activities, rather than require HREC approval for each new activity undertaken

- *Guidelines could be developed by the NHMRC to provide adequate administrative regulation (eg based on the system developed by the NHS incorporating the Caldicott principles) for analyses of electronic data only for the purposes of CA/QA, exclusive of increasing any patient burden or contact, should be considered low risk, even where unconsented, identifiable information is to be disclosed.*

Comments from the HISA Survey

During November 2007 HISA conducted a detailed survey of health informatics professionals, looking at the development of eHealth in Australia. The report resulting from this analysis "A Vision for an Australian Healthcare System Transformed by Health Informatics"¹ looked at Australia's progress toward each of 6 key visions for eHealth, which would combine to deliver a broadly supported and effective eHealth environment. One of these vision areas was privacy, security and confidentiality and the following is an extract from the report in this area:

Section 5: Vision Statement: Managing Privacy Security and Confidentiality

In Australia's fully-enabled electronic information environment designed to engage consumers, transform care delivery and improve population health, consumers have confidence that their personal health information is private, secure and used with their consent in appropriate, beneficial ways. Technological developments have been adopted in harmony with policies and business rules that foster trust and transparency. Organisations that store, transmit or use personal health information have internal policies and procedures in place that protect the integrity, security and confidentiality of personal health information. Policies and procedures are monitored for compliance, and consumers are informed of existing remedies available to them if they are adversely affected by a breach of security. Consumers trust and rely upon the secure sharing of healthcare information as a critical component of high quality, safe and efficient healthcare.

This vision was ranked midway in terms of its difficulty to implement and showed the best alignment of performance to importance. The strategy statements, while still well down in their absolute performance score, were ranked higher than most of the other strategy statements in this study, perhaps reflecting the current level of activity in the public debate on privacy. Respondents felt that engaging both consumers and industry stakeholders in the discussion on privacy was critical to success. The need was to educate these communities on the on the benefits and risks in securely sharing information and engage them in the development of appropriate privacy processes. Collaboration and leadership on these issues throughout government and industry was also considered critical for progress.

¹ A Vision for an Australian Healthcare System Transformed by Health Informatics, HISA Report; November 07:
http://www.hisa.org.au/files/doc/A_Vision_for_an_Australian_Healthcare_System_Transformed_by_Health_Informatics_v8_Public_Release.pdf

Question	Importance (Avg)	Performance (Avg)	Difficulty (Avg)
Question 30: Transparency Policies for the permissible use of personal health information by those other than the patient are clearly defined, accessible, and communicated in an easily understood format. In addition individuals have the right to know how their personal health information has been used and who has access to it.	6.34	3.20	4.68
Question 31: Collection and Use of Personal Health Information Personal health information of the individual consumer is obtainable consistent with applicable federal and state law. It is accurate, up-to-date, and limited to what is appropriate and relevant for the intended use. Consumers have a right to the privacy of their personal health information, taking into account existing exceptions under law. Consumers are apprised when they have a choice in how their personal health information is used and shared and when they can limit uses of their personal health information.	6.34	3.20	4.68
Question 32: Individual Control Individuals are able to limit when and with whom their identifiable personal health information is shared. Individuals are able to delegate these responsibilities to another person. Individuals are able to readily obtain an audit trail that discloses by whom their personal health information has been accessed and how it has been used.	5.76	2.43	4.99
Question 33: Security Measures are implemented to protect the integrity, security, and confidentiality of each individual's personal health information, ensuring that it cannot be lost, stolen, or accessed or modified in an inappropriate way. Organisations that store, transmit, or use personal health information have in place mechanisms for authentication and authorization of system users.	6.49	3.23	4.61

Table 1 - Average scores for importance, performance and degree of difficulty; Managing Privacy Security and Confidentiality

Responses to the strategy statements within this vision focus area are contained in Table 1 . The Survey community believed these issues to be of high importance and low in performance. These strategy statements attracted an average difficulty of implementation score of 4.74, compared to an overall average of 4.86 and were ranked in the middle in terms of their difficulty to implement.

The highest ranking individual issue (in terms of importance was) that of security, and ensuring that information stored was safe from unauthorized access or loss. This is fundamental to ensuring that consumers have sufficient trust in the systems they use to feel confident in using them.

The textual responses were analysed in terms of the primary themes they conveyed and the results are contained in Table 2. On issues that would contribute to our progress toward the stated vision ranked 'Developing Public Knowledge And Debate' as the most important issue. This issue was primarily related to establishing the discussion with health consumers so that have a balanced understanding of the benefits and risks associated with sharing information, and a clear understand of how their information is managed now.

Policy development to control the use of information was also considered important. The creation of secure systems to manage according to established policies was also considered important. As in many of the other strategy areas the broad collaboration across government and those controlling the data was also critical for success.

In regard to the issues that would restrict our progress towards the vision, collaboration and policy development were the two highest ranking themes in the responses, emphasizing that the lack of either of these elements could derail the progress. Leadership was the next highest ranking theme, with the emphasis on the need for leadership within both government and health management to ensure not only the right policies are developed but that there are also effectively implemented. Finally, the broader need for educating the entire stakeholder community was raised, particularly in relation to the value of privacy and the security of the information systems begin proposed.

Type	Theme in comments	% Occurrence
Assisting progress to our the vision	Developing Public Knowledge and Debate	20%
	Policy Development	19%
	Systems Requirements	15%
	Broad Collaboration	9%
Restricting progress to our the vision	Broad Collaboration	15%
	Policy Development	15%
	Leadership	13%
	Developing Stakeholder Knowledge	13%
	Developing Public Knowledge and Debate	13%

Table 2 - Themes appearing in comments from Managing Privacy Security and Confidentiality