Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010

CSC SUBMISSION

CSC Submission

CSC Australia
Health Practice

5 March 2010

PREPARED FOR

Senate Inquiry

SUBMITTED BY

CSC Australia
Lisa Pettigrew, Director Health Services

HEALTHCARE IDENTIFIERS BILL (2010) & HEALTHCARE IDENTIFIERS (CONSEQUENTIAL AMENDMENTS) BILL 2010

SENATE INQUIRY

CSC SUBMISSION

Table of Contents

Table of Contents 2
Background to our Submission 2
Issues under consideration 3
1. Privacy Safeguards in the Bill 3
2. Operation of the Healthcare Identifier Service, including access to the Identifier 3
3. Relationship to national e-health agenda and electronic health records 4

Background to our Submission

CSC made a submission in response to the Discussion Paper on Healthcare Identifiers and Privacy Legislative Proposals in August 2009. The submission was detailed and is attached to this submission. That 2009 submission includes background on CSC and our substantial international experience in assisting governments and health organisations implement national and regional e-health and electronic health records programs.

Please note – CSC agrees to our submission being made public.

This submission should be read in conjunction with our detailed submission provided in August 2009.

Issues under consideration

1. Privacy Safeguards in the Bill

The privacy safeguards are strong and adequate in the Bill.

As Australia embraces e-health, the more complex issue will be the relation of privacy challenges with security procedures across healthcare providers. Clause 27 covers off the security issue satisfactorily, however over time, regulations may be required with greater specificity as to security requirements and standards. Note, we understand NEHTA is undertaking work in this area in relation to development of a Security and Access Framework.

The assignment of an oversight role to the Privacy Commissioner is commendable. However, does the Privacy Commissioner's office have appropriate understanding of clinical relevance and concerns in the delivery of healthcare by health professionals? Anecdotal commentary from practicing clinicians is that they breach the official privacy principles regularly, as the principles are not clinically relevant. Yet most clinicians do earnestly strive to uphold confidentiality of patient details. Involvement of clinical leaders in the review of the operation of the HI Service is recommended.

There is a noticeable absence of detail in the Bill in relation to consent of individuals who want to choose to share their identifier. It is recommended that regulations be considered as to consent for individuals to use and disclose and access their identifiers as they deem appropriate.

Further, it is recommended that in addition to keeping a *private* accurate record of healthcare identifiers and to whom they have been assigned and the information related to the identifier (Section 10, page 8 of the Bill), this 'audit trail' should be transparent and accessible via the internet to the individual concerned, so they can see for what purposes their identifiers have been accessed or shared. For practical purposes, this may be preferable to incorporate into national electronic health records, when fully developed.

Other counties such as The Netherlands have embraced this approach to transparency in relation to access of individual electronic patient health records.

As reflected in our August 2009 Submission, National Privacy Principle 7 remains a problem – the core idea is that the identifiers are eventually used as the primary means of identification for all health systems. To prevent private health providers from explicitly using the Health Identifier as the prime 'key' in their systems will create unnecessary costs and may slow 'uptake'.

2. Operation of the Healthcare Identifier Service, including access to the Identifier

The proposed plans in relation to the operation of the Healthcare Identifier service are satisfactory.

Note that the operational costs mentioned in the Explanatory Memorandum to incorporate use of the Identifiers can be considered part of modernising clinical practice, which are akin to the costs involved for healthcare providers in upgrading medical technology. These costs are not insubstantial; however, they should be considered part of providing a modern and current service.

The penalties do not represent an overall penalty regime and are overly simplistic and lack appropriate sophistication and 'stratification' to reflect the various 'breaches' which may result. See our August 2009 Submission - pages 9 – 10 (our response to Proposal 2).

It is recommended that regulations be considered which include a 'due date' by which healthcare providers must be using the Healthcare Identifiers, or at least a transition time frame.

The mention in the Explanatory Memorandum as to information only being returned when there is an "exact match" is operationally problematic and involves a definitional issue as to what is or can be an "exact match". However, the Bill itself is sufficient in this regard.

3. Relationship to national e-health agenda and electronic health records

The essence of electronic health records is accurate and timely identification of a person and their associated health and medical information to assist with their healthcare.

An accurate, meaningful, efficient, easily understood and universal method for identification of individuals, providers and organisations is essential. The ideal method is assignment of a secure, accurate and unique identifier to all individuals.

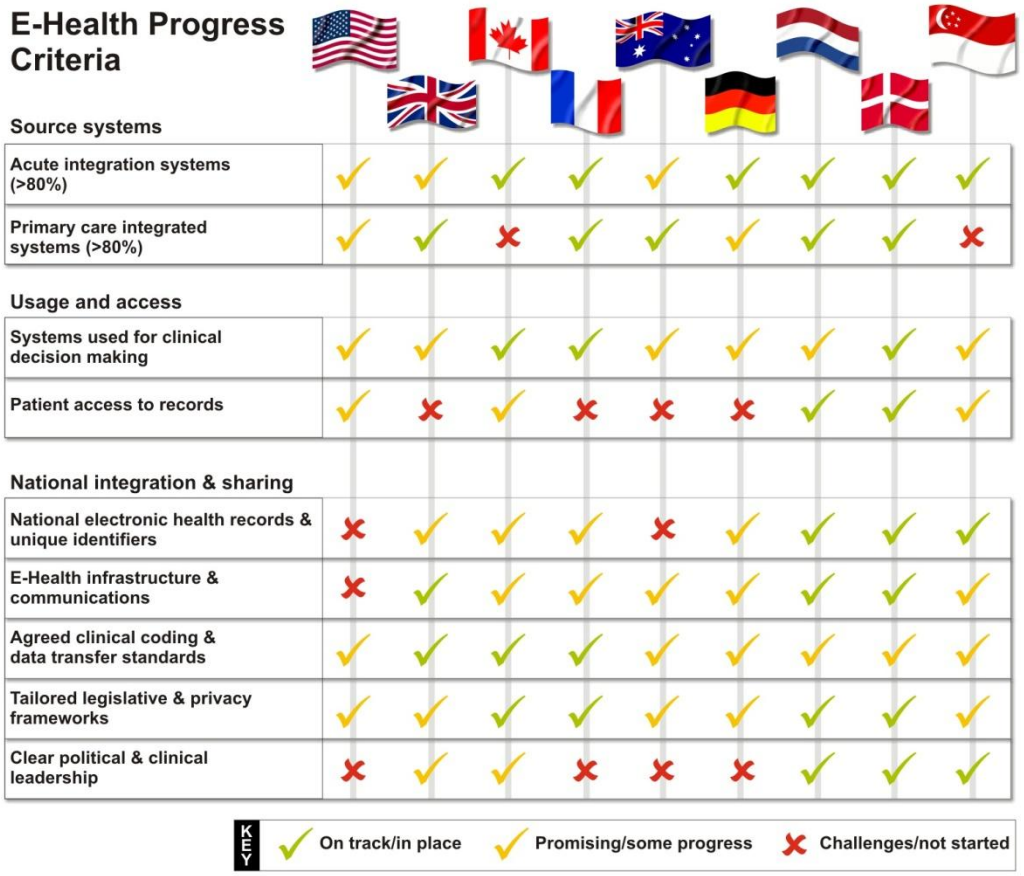
The creation and provision of identifiers as per the Healthcare Identifiers Bill (2010) is essential for Australia to progress on its long overdue journey to embrace e-health and to realise the health outcome goals of electronic health records.

The consent issue mentioned above in response to Question 1 is critical to allowing an individual to choose to link their private or personal health information with their 'official' health information which may be stored in government or health provider systems. For example, individuals may choose to buy or use a private or personal health record (PHR) software application and may want to use their Healthcare Identifier to 'download' their official health information to their PHR and supplement this with additional personal information, such as a health diary.

Relation to international best practice:

One of several key factors in consideration of whether a country can be considered to be advanced in its adoption of e-health and electronic health records is the adoption of unique identifiers coupled with at least eight other criteria.

For a comparison of Australia's international position vis a vis e-health (as at December 2009), see below the CSC Global E-Health Atlas (also accessible at www.csc.com.au/health):



Australia has waited too long for electronic health records for further delays. We commend this Bill to the Parliament for support in order that all Australians can look forward to more accessible healthcare information to assist them and their healthcare providers in improving the health of all Australians.

Healthcare Identifiers & Privacy: Submission based on AHMAC Discussion Paper on Proposals for Legislative Support

CSC SUBMISSION

CSC Submission

CSC Australia
Health Practice

14 August 2009

PREPARED FOR

AHMAC and the Department of Health & Ageing

SUBMITTED BY

CSC Australia
Lisa Pettigrew, Director Health Services

CSC AUSTRALIA
HEALTH PRACTICE

DATE

14 August 2009

ACN 008 476 944 ABN 18 008 476 944

Table of Contents

Table of Contents **8**
Contact Details for Submission: **9**
CSC Australia Contact Details 9
CSC Corporate Details 9
Brief Background on CSC 9
Our Submission **12**
How our submission is organised 12
Section 1 - Our Submission – Answering Your Questions **13**
PART A: NATIONAL HEALTHCARE IDENTIFIERS AND REGULATORY SUPPORT PROPOSALS 13
PART B: PROPOSED NATIONAL PRIVACY REFORMS 26
Section 2 - Our Submission – Further insights on health identifiers & privacy **34**
Clarifying Privacy, Security, Consent & Credentialing 34
Balancing privacy and usability and ease of access 34
Allowing individuals to control their own records 35
Near-Future Trends for Healthcare Records 35
Regular review and assessment of legislative frameworks 36
Sample recent international media and research on related topics 36

Contact Details for Submission:

CSC Australia Contact Details

Ms. Lisa Pettigrew, Director – Health Services
CSC Australia
Ph. 02 9034 2628

CSC Corporate Details

Australian President & CEO: Mr. Nick Wilkinson
National Headquarters: 26 Talavera Road, Macquarie Park, NSW 2113
Ph. 02 9034 3000
CSC ABN: 18 008 476 944
www.csc.com
www.csc.com.au

Brief Background on CSC

Who we are

CSC (Computer Sciences Corporation) is the world's largest health systems integrator. We are a long-standing, global leader in providing technology enabled business solutions and services in many industries globally, particularly the public sector, the defence industry, the resources sector, the banking and insurance sector and, in the USA, Europe and UK in healthcare.

We have over 3,500 staff in Australia servicing clients such as Defence, Department of Immigration and Citizenship, Australian Taxation Office, Centrelink, Rio Tinto, BHP Billiton, Victorian Worksafe, Railcorp and AMP.

Globally, of our 92,000 staff, we have 5,000 professionals dedicated to the health and care sector serving public, private and not for profit providers in all settings, health plans, pharmaceutical, medical device manufacturers and allied industries.

In relation to our experience in healthcare and in assisting with e-health and electronic health record related projects, as part of the United Kingdom's National Health Service (NHS) Program alone, we have delivered:

- over 250 Patient Administration Systems to Acute, Community and Mental Health settings
- 40 Picture Archiving & Communications (PACS) systems storing over 107 million images
- 38 Radiology Information Systems (RIS)
- 28 theatre systems

- 4 maternity systems
- 22 SAP systems (+ 25 into County councils)
- 1,000 General Practitioner (GP) systems
- 71 Child Health systems
- 39 Prison systems and
- 4 Ambulance Emergency Care systems in 196 Ambulances so far.

In the USA, we worked with the US National Health Information Network where we helped lead three of the five pilots to prove the operation and connectivity of electronic health records, applying a standards-based approach to support the 'network of networks' concept.

In Europe we have worked with many countries helping them to create the path for e-health and electronic health records. For example, we worked with the National IT Institute for Healthcare in the Netherlands to build the National Healthcare Information Hub [Landelijk SchakelPunt, or LSP]. This is the "control tower" that enables and ensures the secure nationwide electronic exchange of patient information. Via the hub, healthcare practitioners can request up-to-date patient information from the systems used by other hospitals, pharmacies and GPs.

Our Core Services

Our core services include:

- **Outsourcing** - we manage and maintain IT infrastructures, applications, business processes and systems in a way that improves service levels and reduces costs for our clients. Our services span every requirement: network operations, web and applications hosting, business process outsourcing, data centres, security, hardware and applications management, storage and more.
- **Systems development and integration** - we work with clients to design, build and integrate applications and systems that achieve their strategic objectives. Our commitment to accurate scoping, good governance and delivery of business benefits has won industry awards and customer loyalty. Our services include application development and deployment, systems integration and network planning.
- **Consulting** - CSC's consulting expertise helps organisations to take advantage of new business opportunities and optimize current business performance. Our portfolio covers everything from strategy and business process design to performance and service level management, customer management, supply chain, enterprise solutions, knowledge management, governance structuring, IT architecture, information security, business change and business continuity. We combine these services with in-depth knowledge of many industries, including Manufacturing, Natural Resources, Government and Health.

Examples of CSC's healthcare clients

Some of our Health sector clients with whom we have experience designing and/or implementing national electronic health records, health information exchanges, health identifiers and associated privacy, security, credentialing, authorisation and consent issues include:

- **United Kingdom** – National Health Service
- **Netherlands** - Dutch Ministry of Health, Dutch National ICT Institute for Healthcare
- **Denmark** - Ministry of Health and Prevention and health regions

- **Belgium** - Belgian Ministry of Health
- **Austria** - Austria's four public health insurance agencies (Allgemeine Unfallversicherungsanstalt (AUVA), Sozialversicherungsanstalt der Bauern (SVB), Versicherungsanstalt öffentlich Bediensteter (BVA), Versicherungsanstalt für Eisenbahnen und Bergbau (VAEB))
- **Norway** - Norwegian Ministry of Health
- **USA** – US Office of the National Coordinator for Health Information Technology (ONCHIT)'s National Health Information Network (NHIN) Program
- **USA** - New York State Department of Health – eMedNY (Medicaid)
- **USA** - Carolinas Healthcare System (CHS),
- **USA** - New England Health Exchange Network (now including the MA-Share clinical exchange network)

Our Submission

CSC is pleased to have the opportunity to officially contribute to the discussion on health identifiers, privacy and the related matters of legislative, policy support, security, consent and credentialing.

We would welcome the opportunity for further discussion regarding our submission with AHMC, AHMAC, DOHA and NEHTA.

CSC looks forward to contributing to the e-health discussions and the development and execution of operational plans to make national electronic patient records a reality.

We believe a comprehensive identifier service will support improved quality and safety outcomes and is a significant foundational step towards national longitudinal health record capability for Australia. Further, this service needs to be operating within a robust and federated access control framework to deliver full benefit to the Australian healthcare sector. The larger framework is not yet evident and we look forward to contributing in its design, evolution and development.

Further, we endorse most of the content of recent national strategies and reports for e-health, however we note that the 'next step' is to develop and agree appropriate 'operational models' for e-health. The recent initiatives and statements regarding when Australia may have person-controlled electronic health records and when we may have identifiers, is positive. Yet the recent reviews still do not address fundamental issues of how will the practise of medicine and patient care change – what is the new operational model for healthcare when we do have electronic records, whether they are controlled by patients or otherwise.

We believe there are legitimate reasons why these initiatives, and technology change in general, is more challenging in healthcare than other industries, and will be producing materials on these issues in coming months.

How our submission is organised

Our response is primarily divided into two main sections:

- **Section 1**
    - We answer the questions posed in your paper '*Healthcare identifiers and privacy: Discussion paper on proposals for legislative support*' and we comment on your specific proposals.
- **Section 2**
    - In section 2, we highlight some other insights regarding these matters which we believe may be useful to your deliberations, including examples from overseas, where not previously included in our response.

Section 1 - Our Submission – Answering Your Questions

PART A: NATIONAL HEALTHCARE IDENTIFIERS AND REGULATORY SUPPORT PROPOSALS

Introduction from the Discussion Paper

Feedback is sought on whether the proposals for legislation:

- **are fit for purpose and support the objectives of the HI Service**
- **will raise any significant issues for stakeholders if they are implemented as proposed**
- **need modifying or adding to in order to support implementation of the HI Service and participation by individuals, healthcare providers and healthcare provider organisations.**

Proposal 1:

Provide Medicare Australia with functions, in or under Commonwealth legislation, to establish and operate the HI Service for the purpose of accurately and uniquely identifying healthcare individuals, healthcare providers and provider organisations and enable communication between individuals, healthcare providers and provider organisations. The functions would be conferred on the Chief Executive Officer of Medicare Australia and cover:

- **assigning, collecting and maintaining identifiers to individuals, individual healthcare providers and organisations including by using information it already holds for existing purposes**
- **developing and maintaining mechanisms for users to access their own records and correct or update details**
- **collecting information from individuals and other data sources**
- **use and disclosure of these identifiers and associated data, including personal information, for the purposes of operating the HI Service.**

Key Stakeholder Questions about providing functions to operate the HI Service:

Q1. Do you agree that the functions to be conferred on the Medicare CEO are sufficient?

CSC Response

E-health represents a new industry and an entirely new business model and process model for healthcare. We are only at the beginning of this journey and no one can predict exactly where the journey will take us as a nation, in terms of new ways to deliver and receive healthcare. We should not approach legislative change as 'more of the same' or an incremental improvement or modification to current arrangements, but rather part of the structural reform of healthcare.

We support the position that the legislative design reflects pragmatic and sensible arrangements to support a rapid initiation of e-health related activity given current arrangements. However, it is essential that legislation does not 'lock in' to current governmental arrangements that may limit flexibility.

CSC proposes that the functions outlined for establishing and operating the HI Service, for the stated purposes, be embodied in **a new role to be created in the legislation for a National Health Information Registrar**. This role would have particular responsibilities in relation to the management and oversight of the HI Service and in particular, management of the likely queries from the public and healthcare providers in relation to the access arrangements for their identifiers. This role would have all the functions outlined in Proposal 1.

The National Health Information Registrar would be a new role, but it should not, and need not, be a new job in the first instance. The role of National Health Information Registrar, should, in the first instance be given to the CEO of Medicare.

CSC therefore endorses the functions and powers of the National Health Information Registrar being conferred to the CEO of Medicare. We note that some current Medicare organisational procedures, policy and culture may not be applicable to the health identifier service.

Creating the role of National Health Information Registrar allows the flexibility to adapt to machinery of government changes. The creation of the new role also allows the flexibility to adapt to the expected uptake of e-health solutions and services and the possible subsequent increasing workload associated with queries from the public and the healthcare providers which may require, over time, for the Registrar role to become an actual stand-alone job.

Further, we envisage that the development and use of electronic patient health records may require additional functions separate from the functions outlined above. Functions are likely to be required for oversight or ombudsmen-like responsibilities to allow for independent consideration of issues and queries from the public.

Proposal 2:

Where an IHI or HPI-I is associated with health information about an individual, the collection, use and disclosure of an IHI or an HPI-I will be subject to the privacy and health information laws applicable to that health information.

Misuse of an IHI or HPI-I by a healthcare provider will be able to be pursued as a breach of privacy in jurisdictions with privacy laws or will be subject to other penalties set out in relevant health records or health service legislation.

Key stakeholder questions about application of general privacy and other laws:

Q2. Are there significant issues raised by regulating the handling of healthcare identifiers by public and private health sector organisations through existing privacy and health information laws with some additional regulatory support through specific enabling legislation for healthcare identifiers?

CSC Response

We believe further discussion and consideration is required around health identifiers and health information regarding wilful or intended breaches of privacy as opposed to accidental, unintended breaches of privacy.

The above proposal may be achieved by existing legislation, and so specific provisions to affect it may be unnecessary. However we believe some case studies and examples will be required to facilitate community consultation, to educate and inform citizens and health providers about may be appropriate and inappropriate and what is legal and what may be illegal.

The challenge of truly protecting privacy is not unique to the health industry and will continue to be problematic. We believe it is worth clarifying privacy as opposed to security issues. The two are

intertwined as security measures, processes and systems are often needed to safeguard the privacy of particular information. A breach of security can lead to a breach of privacy – intended or unintended.

A breach of personal privacy in any industry is hard to compensate for, or 'take back', whereas a breach of security can often be compensated for, and the offending breach can be remedied.

It is important and necessary to legislate as proposed above to prevent misuse, however, there will need to be a clear definition of what constitutes misuse – and what "exceptions" are defined *in extremis;* there will also need to be a question of restitution and what actionable steps can or should be taken when breaches are detected and whether there is a role to proactively identify breaches or whether a reactive model of responding to complaints is sufficient.

Our experience is that currently, in many healthcare settings around Australia, there is great respect for the *privacy* of patient and provider data but in some instances there may not be adequate *security* procedures and processes for protection of information. Guidelines and guidance on security processes and procedures will be required as start to make extensive use of health identifiers and the associated personal health information.

As an example, sharing of passwords is common in many industries, including health. This sort of 'breach' is accepted and forgiven as part of 'doing business efficiently' as it is sometimes perceived as too cumbersome, costly or awkward to put in place appropriate security that is also user-friendly and timely. In small businesses, some security procedures may not exist as they may not be deemed required, based on current business and clinical processes for sharing information (which may only be partially automated) amongst a small number of authorised people.

To answer the question above about the adequacy of privacy legislation and breaches, some categorisation of breaches would be useful and public debate on the breaches is required to elicit input from the public and to assist in education of all stakeholders as to the implications of a privacy breach in relation to health information. For example, a possible hierarchy of penalties could involve:

Level of severity	Example of privacy breach
Lower levels of penalty	• Inadvertent breach of privacy which could not be avoided – individuals who may have had access to information anyway are provided access (eg., other health professionals) • Inadvertent breach of privacy which could have been avoided (eg., lack of computer or printer security)– individuals who may have had access to information anyway are provided access (eg., other health professionals) • Inadvertent breach of privacy which was accidental but could have been avoided (eg., lack of computer or printer security or poor data maching)– individuals who may would not have had access to information anyway are provided access (eg., other members of the public)
Highest levels of penalty	• Inadvertent breach of privacy which was not accidental, could have been avoided and should have been foreseen and may breach other security obligations (eg. sharing of passwords or computer access) • Intended breach of privacy by health professional/health sector employee • Intended breach of privacy by breach of security

In addition, a hierarchy of penalty should also consider whether there is a differentiation of penalty for a singular breach (disclosing one IHI) as opposed to simultaneous multiple breaches (disclosing thousands of IHIs).

However, it is important that administration of health identifiers, particularly IHIs, not become cumbersome or administratively complex.

Key stakeholder questions about application of general privacy and other laws:

Q3. Are there circumstances where penalties for misuse of a healthcare identifier and associated information that is held by a healthcare provider will be inadequate?

CSC Response

This question requires some 'real life' examples to enable appropriate debate. See also our response above to question 2.

It is also worth noting that the privacy issues in respect of an identifier service which contains no clinical information are significantly more straightforward than they are for the use of identifiers to support individual electronic health records (IEHRs).

In relation to electronic health records, there may be ethics issues to be considered here in relation to whether a healthcare provider or health professional may breach privacy in order to deliver the best possible care, as opposed to a wilful breach, unrelated to patient care.

In the case of individual health identifiers (IHIs), the service itself, as we understand, is not anticipated to ever return any demographic data, so there are no substantive privacy issues at that level. The use of the identifiers in the field does open up some possible issues, but the general operation of the identifier service in the absence of IEHRs are such that the risk exposures are not materially different from those that exist at present.

Proposal 3:

Definitions of healthcare service and healthcare service provider will be included in the legislation.

Key stakeholder questions about definitions:

Q4. Is it appropriate that definitions contained in privacy law are adopted?

CSC Response

Yes, definitions should be included and consistency should be sought with other health related Acts and Regulations. In particular, there should be harmony with the new plans for NRAS.

The lack of straightforward and broadly applicable definitions of what constitutes a healthcare service and a healthcare service provider has been an issue for the healthcare sector for some time. As an increasingly national-level orchestration of healthcare delivery evolves, the present situation of multiple overlapping, and sometimes contradictory, definitions of provision are become an increasing hindrance to developing workable business solutions. See also answer below question 5.

Key stakeholder questions about definitions:

Q5. Are there other specific terms that should be defined?

CSC Response

There are some other matters and terms which may require inclusion, clarification and definition:

- The **manner and method by which a healthcare service is delivered** will increasingly become important and requires definition. The recently released National Health & Hospital Reform Commission (NHHRC) Final Report highlighted that there will increasingly be new ways of delivering care which government must plan for, such as telemedicine and virtual consultations. These modern and technologically supported modes of care delivery necessarily require support by health identifiers and associated authentication services
- There will be a new and growing discipline and industry around **health information and identifier management**. This new discipline should be treated in a similar fashion as healthcare service with respect to authorised use of healthcare identifiers; to this end, healthcare information and identifier management should be an authorised use of data and should include data quality assurance activities including data matching and reconciliation, integration of new information and new healthcare providers and systems and these activities should be recognised as fundamental to professional health services
- Definitions regarding the **status of health information attached to or accessible via an identifier** may be required – that is, clarifying 'official' data, entered by a health professional in a certified health IT system, as opposed to information or data that has an 'unofficial' status and may not be validated
- **Who or what issues the health identifiers?**
- **Who or what (if anyone or any organisation) owns the health identifiers?**
- It is worth noting that the **idea of a health identifier for individuals itself does not represent 'new' data**; there are currently health identifiers for individuals in almost all health IT systems. This proposal is for a nationally standard set of health identifiers. If health providers cease to use any paper records, this should be an acceptable practice (see case studies for some examples of this and the implications for some patients).
- What **forms can the physical representation of the IHI take**? Is it written on a piece of paper? Embedded in a digital certificate? Printed on a letter? Embossed on a card? Verbally recited? Is the IHI like a TFN which can be 'quoted'? Or is it like a credit card number which is always represented in the physical card form or, where the card cannot be viewed, must always have other verification information associated with it?
- Other national identifiers – the definition of the health identifier for organisations requires further clarity, not only for privacy reasons. Is the heath identifier for organisations a legal entity identifier? For example, akin to an ABN? Or is the organisational identifier an address identifier? Do we need a further address or location identifier to associate with health identifiers for organisations and individual provides? Further, as the number and variety of medical technology devices incorporating healthcare information increases, identification of devices which may involve health identifiers will require consideration, and definition.

Proposal 4:

The HI Service Operator will only disclose an individual's IHI and the minimum personal information required to identify an individual to an authorised healthcare provider. Requests for an IHI must be supported by a minimum set of personal information.

Proposal 5:

Healthcare providers will be authorised to use or disclose an individual's name, date of birth, sex and address details in order to request an IHI from the HI Service Operator.

Proposal 6:

The HI Service Operator will disclose information held in the Service only to authorised users. The term 'authorised user' will be defined in the legislation.

Proposal 7:

The HI Service Operator will be authorised to disclose the HPI-I and relevant data fields for professional registration and other purposes to bodies set up in legislation establishing the NRAS.

Proposal 8:

Secrecy provisions similar to those set out in the Health Insurance Act or the National Health Act would apply to the disclosure of information by staff in undertaking the HI Service Operator function.

Proposal 9:

Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to secondary uses and disclosures of HI Service information.

Key stakeholder questions about use and disclosure:

Q6. Do the limits on disclosure set out in Proposal 4 provide adequate protection for an individual's personal information?

CSC Response

This is a prudent set of limits for the purpose of obtaining an IHI while maintaining the privacy of the information underpinning the identifier. On a related point, proposal 4 will in general be adequate, but the requirement for disambiguation in some cases should be explicitly recognised.

We perceive some potential confusion in this proposal between providing an IHI and the return of personal information versus providing personal information in order to get the IHI in return.

The business process models for how electronic health identifiers and the associated information are to be accessed is not clear and may not yet be defined. Regardless of the technology solution for how anyone accesses health identifiers and/or the associated information, we recommend strong logging and audit trail capabilities are embedded in all health IT systems providing access to health information. Electronic audit trails should store information on who accessed data, when and why and whether the information was shared with others. Modern technology solutions can automatically capture and store this data without additional information being required by the user.

There are technology solutions that can assist in realising and implementing privacy policy, once the policy is confirmed. It is not always necessary for the HI service to store any personal health information data.

For example in the Netherlands the Dutch National IT Institute for Healthcare) adopted a pragmatic, secure national information hub to promote information exchange among medical practitioners and address a steep rise in healthcare costs. The resulting system, Landelijik Punt (LSP), protects patient privacy and uses a series of standard interfaces to give healthcare providers access to complete patient histories – even if data is stored on different provider systems.

The LSP has made it possible for the Dutch to introduce a secure national system despite their fragmented landscape and the structural limitations. Delivered by CSC in 2006, it isn't a database or even a "system", but a pioneering interface that pulls records from multiple healthcare providers to create a

more complete record of individual patients. Importantly that bundle of information can only be held for 24 hours, and not copied or saved. The healthcare provider is the 'keeper' of the information and the patient has the right to see the information and to make comments. The system has a number of security features: a Java card authenticates physicians' identities; neither LSP nor the doctors' systems store retrieved files; and doctors can only see information that patients have previously granted them access to. And to address privacy concerns, patients can access a web portal that shows the organisations and locations where their information is kept, as well as a log of what information has been accessed, when and by whom.

Alternatively, in 'source systems' such as electronic medical records used in hospitals by clinical staff, the IHI may be stored but may not be the main identifier used to identify patients and their health information.

A further policy question raised by this proposal is anonymity. Will the legislative framework and/or clinical care policies allow patients to request anonymity?

Key stakeholder questions about use and disclosure:

Q7. Is the authorisation for healthcare providers set out in Proposal 5 required to provide certainty to healthcare providers, noting that the use or disclosure could occur under existing privacy arrangements as a directly related and reasonably expected secondary use or disclosure of health information?

CSC Response

This proposal is necessary and pragmatic. The integrity of the health identifiers relies on matching information on the same person to the same identifier. In order to match records and identities, there has to be information to match to, so pragmatically this information has to be available to use a proposed.

We note that in our experience, data matching can be a complex and critical task. Occasionally further information above the basic demographic information may be required to confirm the identity correctly.

Key stakeholder questions about use and disclosure:

Q8. Does the limit on disclosure set out in Proposal 6 provide adequate protection for a healthcare provider's personal information?

CSC Response

Yes, information should only be provided to 'authorised users' (to be defined), however we propose adding in that information is to be provided to authorised users for 'authorised purposes'. Presumably the technology solution supporting the HI service will include strong system-to-system authentication and confidentiality mechanisms.

Please also refer to our comments above regarding security practices, the HI service may be meeting its obligations and abiding by the law with respect to privacy and confidentiality, yet, once the information is provided to an authorised person, some guidance on what that person can then do with the information may be required. An appropriate metaphor here may be a house with a very secure front door but no security on the backdoor or windows.

Key stakeholder questions about use and disclosure:

Q9. Does the proposal to apply secrecy provisions similar to those set out in the Health Insurance Act or the National Health Act provide sufficient protection for personal information held by the HI Service Operator?

CSC Response

Yes, we support this proposal. We note that the penalty structure may require review subsequent to community and clinical consultation.

Key stakeholder questions about use and disclosure:

Q10. Is there a need to apply a specific penalty to unauthorised use or disclosure of healthcare identifiers by health sector or other participants who hold the healthcare identifier in association with health information?

CSC Response

Yes, we believe the penalty structure requires review and consideration given to different penalties for different types of disclosure taking the conditions and reasons, if any, into consideration and also taking into consideration the implications or consequences of inappropriate disclosure of healthcare identifiers or associated information.

We note that the identifier numbers should not be "published" or shared in any broad sense, however, these numbers will necessarily be disclosed in a whole host of ways and means as they are used to operate national electronic health records, for example, printed on documents which may need to be manually handled. It is impractical to keep the numbers totally undisclosed.

Notwithstanding this point, unauthorised use of a health identifier should be regarded as a serious issue, where it can be proven.

Key stakeholder questions about use and disclosure:

Q11. Do you agree that existing health information regulation and administrative arrangements will provide sufficient secondary use requirements for organisations handling healthcare identifiers?

CSC Response

In principle we agree, however we concur with the Office of the Privacy Commissioner's submission last year to NEHTA suggesting that further detail is required as to how secondary use is to be managed, particularly for uses beyond that of medical research.

If there is ambiguity and conflict in existing regulations, this should be harmonised.

Proposal 10:

Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to data quality.

Key stakeholder questions about data quality:

Q12. Do you agree that existing health information regulation and administrative arrangements will provide sufficient data quality requirements for organisations handling healthcare identifiers?

CSC Response

If this question is in relation only to the health identifiers, then the primary data quality issue is the integrity of the number. However, if this proposal is a broader question in relation to data that may be attached to or accessible via the identifiers then we believe further guidance is required in relation to data quality. In particular, we believe incentives are required to encourage data quality activity by all users including clinical staff. See case studies below for information on incentives in the UK.

We also note that data quality measures and guidance must encompass issues of omission, commission and timeliness. As the health system and health industry comes to rely on electronic records, merely identifying data quality issues will be inadequate. Data quality issues such as incorrect or missing information must be addressed in a timely fashion.

Your paper indicates that Medicare Australia's existing information and 'evidence of identity' processes will apply. The current arrangements for the Medicare number were not originally designed to be as strict as the anticipated IHIs, hence, the verification and matching undertaken for the HI service may need to be stricter than current processes and demand for transparency around these rules may increase.

Proposal 11:

Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply for data security.

Key stakeholder questions about data security:

Q13. Do you agree that existing health information regulation and administrative arrangements will provide sufficient data security requirements for organisations handling healthcare identifiers?

CSC Response

Yes, current arrangements are likely to be sufficient; however, the fact that a new identifier framework will be introduced may require some reinforcing of existing arrangements, for example, to avoid 'joining up' otherwise separate electronic information in separate datastores. Further, the advent of electronic health records may mean greater electronic interaction between private and public sector health systems and provisions may need revision in light of this increased interaction.

Further, to facilitate the appropriate use of identifiers and to foster an environment conducive to public acceptance and usage of electronic health records, the agencies involved (such as Medicare Australia) should take an enabling view of their statutes, rather than primarily a restrictive view.

Proposal 12:

Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to openness.

Key stakeholder questions about openness:

Q14. Do you agree that existing health information regulation and administrative arrangements will provide sufficient openness requirements for organisations handling healthcare identifiers?

CSC Response

Yes, there is sufficient openness, although a governing body such as AHMC or AHMAC may need to administer compliance with the requirements in a more coordinated way across the federated network. As noted above, agencies should take an enabling view of the statutes.

Proposal 13:

Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to access and correction. No additional legislative requirements will be developed for access and correction.

Key stakeholder questions about access and correction:

Q15. Do you agree that existing health information regulation and administrative arrangements will provide sufficient access and correction capability for individuals?

CSC Response

Yes and our experience with electronic health record programs in other counties suggest that it is very important for the regulation and administrative arrangements to be matched by equivalent technology delivery. For example, individuals must have easy access via online self-service tools to allow for access and corrections.

Proposal 14:

It is proposed that Commonwealth legislation provide that NPP 7 does not apply to the adoption, use and disclosure of the IHI or the HPI-I by private sector healthcare provider organisations for the purposes of accurately and uniquely identifying individuals and individual healthcare providers respectively for health information management and to enable communication between individuals, healthcare providers and provider organisations.

Proposal 15:

It is proposed that Commonwealth legislation will provide that NPP 7 does not apply to the use and disclosure of Medicare numbers to Medicare Australia by private sector healthcare provider organisations for the purposes of the retrieval of individual identifiers.

Key stakeholder questions about identifiers:

Q16. Will the proposals to overcome current identifier restrictions on private healthcare providers effectively enable participation in the HI Service?

CSC Response

Yes, we agree that as a minimum NPP 7 should not apply as proposed. In fact, the basis for NPP 7 needs to be reviewed and reconsidered as the *purpose* of a program to create and use national electronic health records is explicitly to do some of the things currently prohibited by NPP 7.

There are a great many incentives required to enable and encourage appropriate participation by private healthcare providers and insurers in the HI service and in use of national electronic health records. The proposals above are supported as a good start.

It is also worth noting that these provisions are important for IT companies involved in designing and implementing IT systems to support electronic health records for the public and private health industries. We look forward to further detail.

Key stakeholder questions about identifiers:

Q17. Do these proposals raise any significant issues in relation to the handling of identifiers?

CSC Response

We support these proposals but we believe they raise significant issues as they do not go far enough in clarifying the arrangements for use of identifiers. NPP 7 in particular is substantially problematic in its premise – it needs substantial revision to support the purpose of national electronic health records which is to explicitly share information.

Further issues are raised for companies that 'handle' but do not necessarily access health information. For example, companies like Google and Microsoft offer (not yet in Australia) products that can store personal electronic health record data for personal access by individuals. The companies themselves do not access the data, they are providing their technology as a tool for individuals to use to access their *own* health data. Review of the privacy principles will require consideration of these new technology developments and the use of government-issued identifiers which will be fundamental to allowing and arranging for individuals to access their health data.

Proposal 16:

Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to anonymity.

Key stakeholder questions about anonymity:

Q18. Do you agree that existing health information regulation and administrative arrangements will provide sufficient anonymity requirements?

CSC Response

Current provisions will need to be checked against the emerging international consensus on this issue.

There are two concepts bound together – anonymity and optionality. As an individual, I may or may not choose to remain anonymous at different points in my life at times when my health needs change. This should not pose a policy issue, and as healthcare technology develops, this sort of 'functionality' can be enabled to support the policy.

As stated above, an operating model is required here to assist healthcare providers in understanding what to do when patients request or require anonymity. Is service denied? Are they allowed anonymity now or previously when records were not electronic? What are the alternative means for verifying identity and if data is stored then how is it accessed for a person requesting anonymity.

Depending on the reasons for individuals requesting anonymity, we believe strong logging and audit trail functionality built into health IT systems can greatly assist in providing comfort to individuals who may be concerned about breaches of their privacy. Existing anonymity provisions need to remain for issues of personal safety for particular individuals.

Proposal 17:

Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to transborder data flows.

Key stakeholder questions about transborder data flows:

Q19. Do you agree that existing health information regulation and administrative arrangements will provide sufficient requirements for transborder data flows?

CSC Response

There are issues in transborder flows, particularly with the NSW legislation, which we understand to be very restrictive. National statutes to harmonise or override variance in state legislation may be necessary.

As stated above, we should not approach legislative change as 'more of the same' or an incremental improvement or modification to current arrangements, but rather part of the structural reform of healthcare, particularly in this area of electronic exchange of data.

With the rise of international mobility and medical tourism it is likely this area of statute may need updating to accommodate interstate but also international data flows as a regular occurrence rather than an exception.

Key stakeholder questions about transborder data flows:

Q20. Does this proposal raise any significant issues in relation to the handling of identifiers?

CSC Response

Yes, as your paper states, Australia's current privacy landscape is fragmented and complex. We do not believe it is useful to talk only of transborder or privacy issues in relation to identifiers, the discussion must be about the healthcare information which is likely to be attached and/or accessible via the identifier.

There are significant issues in relation to the use of the identifiers and their handling but not the identifiers themselves. To support the evolution of national electronic health records, there must be nationally consistent supportive privacy legislative and well understood and 'implementable' protections.

Proposal 18:

The role of the Ministerial Council would be set out in an intergovernmental agreement. Key elements would be set out in legislation, including any processes for future consideration by the Ministerial Council about the operation or expansion of functions of the HI Service.

CSC Comment

We agree.

We further encourage alignment and harmony between the work being undertaken by the ALRC and the Ministerial Council's proposed improvements to privacy legislation and arrangements governing health related information. Disharmony between the Attorney-General and Health portfolios will hamper private and public sector investment in the construction and use of electronic health records.

Proposal 19:

Establish a process for controlling the expansion of the future uses of the HI Service. This could be done by:

• providing for the Minister who is responsible for the legislation to determine future operation or expansion of the service subject to a requirement to undertake a privacy impact assessment and seek agreement from all state and territory Health Ministers.

Guidelines for the steps to be undertaken would be expected to be set out in the legislation.

CSC Comment

We challenge the part of Proposal 19 which suggests that decisions regarding the expansion of the HI service is primarily governed by the Federal Minister and State Ministers. This group, including all state Health Ministers collectively over-represents the public sector acute health setting and does not adequately include patients and consumers. For the HI service and the entire concept of national electronic health records to be successful, engagement of the primary health sector and the private provider sector must be paramount. Further, it is not unrealistic to envisage Federal and State Ministers not always coming to agreement regarding expansions to the HI Service.

We suggest the Federal Health Minister has responsibility for the legislation to determine the future operation or expansion of the HI service and the Federal Minister *consults with* all state and territory Health Ministers and CEOs or equivalents of private health providers, peak health service delivery bodies and peak consumer and patient groups.

Proposal 20:

It is proposed that these functions would be undertaken by Medicare Australia in its role as the initial HI Service Operator (see Proposal 1 above).

CSC Comment

As above, we support these functions being allocated to the new role of the National Health Information Registrar and then delegated to Medicare Australia.

Key stakeholder questions about participation agreements:

Q21. Do you think participation agreements are an appropriate mechanism for setting out the responsibilities of the parties involved (i.e. healthcare provider organisations and the HI Service Operator)?

CSC Response

Yes, as we proposed above, we endorse participation agreements. Industry and public consultation in a structured format will be helpful.

See Section 2 for international case studies.

Key stakeholder questions about participation agreements:

Q22. If so, do you consider that legislation is necessary to underpin the participation agreements?

CSC Response

We do not believe at this stage of development of national electronic health records that participation agreements need to be underpinned by legislation. In fact, legislation may inadvertently prescribe certain participation and consultation approaches. We suggest that participation agreements evolve through innovation and collaboration within the industry.

In the future, once Australia reaches a point of 'critical mass' of electronic health record adoption, it will be appropriate to review the legislation is required to confirm appropriate ongoing participation and consultation agreements.

Proposal 21:

It is proposed that existing Commonwealth, state and territory privacy and/or health information regulatory arrangements will apply.

CSC Comment

We believe this proposal is sensible and efficient. We note that if there is a conflict between state and commonwealth statutes, a pragmatic response would be for the Commonwealth position to apply.

PART B: PROPOSED NATIONAL PRIVACY REFORMS

B.1 A national privacy framework (incorporating health-specific requirements)

Key requirements for national health privacy regulation are:

• recognition of the need to provide specific regulation for health information to appropriately balance the particular sensitivities of this type of information with the benefits of its availability for healthcare and other public interest purposes

• support for national e-health initiatives by a national health privacy framework that is, to the greatest extent possible and appropriate, uniform

• involvement of Health Ministers in decision-making processes in recognition of their responsibility for health policy and service delivery

• implementation of a national health privacy framework in a timeframe that supports national e-health investment and implementation, in particular healthcare identifiers.

These requirements can be addressed through arrangements that are established for implementation of the national framework, its oversight and administration, coverage of the law, definitions that relate to health information and some technical amendments to the UPPs.

Your feedback is sought on the potential impact on people who deliver and receive healthcare of the changes proposed in the areas of coverage, definitions and amendments to the UPPs.

CSC Comment

We endorse the requirements above. However, the only reference to consultation in the requirements is for Health Ministers to be involved "in recognition of their responsibility for health policy and service delivery'. We agree that Ministers must be included; however we note that some other very important

stakeholder groups are omitted from the requirements – we suggest that involvement of healthcare providers and patients be explicitly included in this set of requirements.

Further, as stated above, we support the position that the legislative design for a new privacy framework reflect pragmatic and sensible arrangements to support a rapid initiation of e-health related activity given current arrangements. The framework must be 'implementable'.

We would also suggest that the requirements include the review of the privacy framework for the health industry at regular intervals to ensure our legislative arrangements "keep up" with technological developments and citizen attitudes to access and sharing of health information.

Proposal 22:

National legislation include requirements such as: conciliation being a critical element in the approach to resolving complaints; an independent administrative or judicial mechanism; the length of time consumers have to lodge a complaint; powers of regulators; and sanctions for breaches of the law by agencies or organisations.

Guidelines including minimum standards be developed and agreed to by regulators to ensure that there is a consensus in the way in which privacy laws are to be applied across Australia.

Jurisdictional regulators be empowered to jointly determine a common approach to applying these minimum standards.

Key stakeholder questions about administration of a national privacy framework:

Q23. Are there any other requirements that should be specified in legislation?

CSC Response

We believe these inclusions are a substantial start to privacy legislation pertinent to supporting electronic health information.

Key stakeholder questions about administration of a national privacy framework:

Q24. Is it necessary that arrangements for and enforceability of directions or guidelines that are jointly agreed by privacy regulators to be supported by legislation?

CSC Response

The powers of the privacy regulators should be reflected in legislation.

Proposal 23:

Health information of deceased individuals should be subject to the same protection as other personal information about deceased persons whether this is through privacy law or other arrangements.

Key stakeholder questions about deceased persons:

Q25. Are there any reasons for the privacy of health information about deceased persons to be treated differently to other personal information about them?

CSC Response

No comment.

Proposal 24:

Include a definition of 'health service provider' as 'an organisation that provides a health service to the extent that it provides a health service'.

Key stakeholder questions about definitions:

Q26. Is the proposed definition of health service provider appropriate?

CSC Response

No, this description is inadequate.

Key stakeholder questions about definitions:

Q27. Are there any other terms that need to be defined to support a health information privacy protection as part of a national framework?

CSC Response

See response above to question 5.

Proposal 25:

Amendment of 2.5(c) to allow the collection of sensitive information where there is a serious threat to an individual's welfare.

Proposal 26:

Deletion or modification to 2.5(d) to exclude the right for non-profit organisations to collect health information about their members.

Proposal 27:

Amendment of 2.5(f) to provide that any guidance issued by the Privacy Commissioner in relation to the collection of sensitive information necessary for research purposes be required to be developed in conjunction with input from other appropriately qualified individuals or organisations in the field of research.

Proposal 28:

Any rules or guidelines issued by the Privacy Commissioner in relation to the collection of identifying health information where it is necessary for the funding, management, planning, monitoring or evaluation of a health service be developed in conjunction with input from other appropriately qualified individuals or organisations in the health service management field.

Key stakeholder questions about UPP2 - Collection:
Q28. Do you agree that the amendments proposed above are appropriate?

CSC Response

These are sensible and pragmatic proposals.

Key stakeholder questions about UPP2 - Collection:

Q29. Are there any other circumstances where the collection principle might require amendment in relation to health information?

CSC Response

This appears to be a suitable list.

Proposal 29:

Amendment of 5.1(c) to allow the use or disclosure of sensitive information where there is a serious threat to an individual's welfare.

Proposal 30:

Amendment of 5.1(f) to provide that any guidance issued by the Privacy Commissioner, in relation to the use or disclosure of sensitive information is necessary for research purposes, be required to be developed in conjunction with input from other appropriately qualified individuals or organisations in the field of research.

Proposal 31:

Rules or guidelines issued by the Privacy Commissioner in relation to the collection of identifying health information where it is necessary for the funding, management, planning, monitoring or evaluation of a health service be developed in conjunction with input from other appropriately qualified individuals or organisations in the health service management field.

Proposal 32:

An exception is proposed to allow personal information to be used or disclosed by an agency or organisation where an individual is known or suspected to be missing or deceased, subject to this not being contrary to any wishes expressed by the individual before they went missing or became incapable of consenting, with disclosure limited to a law enforcement officer for the purposes of ascertaining the whereabouts of the person.

Proposal 33:

It is proposed that the definition of a 'person responsible for an individual' be altered to provide for:
• any person who has a personal relationship with the individual rather than only a person who has an intimate relationship, or
• a person who is responsible for providing support or care to the individual rather than only the person who is primarily responsible.
Guidelines could identify the grounds on which a personal relationship exists or that a person is responsible. These would include such things as whether there is a sufficient degree of intimacy

or level of responsibility. Another alternative would be to set the list up as an inclusive rather than an exclusive list.

Key stakeholder questions about UPP5 – Use and disclosure:
Q30. Do you agree that the amendments proposed above are appropriate?

CSC Response

Yes

Key stakeholder questions about UPP5 – Use and disclosure:
Q31. Are there any other circumstances where additional guidance about the use or disclosure of information would be helpful?

CSC Response

This appears to be a suitable list.

Key stakeholder questions about UPP5 – Use and disclosure:
Q32. In relation to Proposal 32, should an agency or organisation be required to have a reasonable expectation that the person responsible for the individual will act in the best interests of the individual in receiving that information? Would guidelines provide sufficient certainty?

CSC Response

No comment.

Proposal 34:

The consent of individuals is required to the use or disclosure of health information for direct marketing purposes.

Key stakeholder questions about UPP6 – Direct marketing:
Q33. Do you agree that the consent of the individual should be obtained for the use or disclosure of health information for direct marketing purposes?

CSC Response

Further clarification on 'direct marketing' is required here. Overseas experience suggests that effective and useful chronic disease management programs can be created and managed by private or public health organisations. These programs can often improve the health of the individuals 'enrolled' in the programs and can reduce public and private healthcare expenditure by assisting patients with proactive care management. To enrol patients or members in these programs a type of 'direct marketing' may be required. Privacy legislation should not prevent this sort of program which can be considered as an extension of both prevention and/or outpatient-style services.

Proposal 35:

Guidelines be developed by the Privacy Commissioner outlining key requirements for retaining health information (e.g. minimum retention periods and obligations owed by a healthcare provider to an individual where a healthcare service has been sold, amalgamated or closed).

Key stakeholder questions about UPP8 – Data security:
Q34. Are guidelines sufficient to ensure that health information is retained for a suitable period of time?

CSC Response

We would propose that health information is retained as long as possible to assist with both individual care and population research and care. However, an important implementation consideration is storage arrangements for the retained information, whether stored in paper or electronic form.

Proposal 36:

It is proposed that the exception from providing access to health information where providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations does not include negotiations about provision of health services.

Proposal 37:

A note be inserted into the Access and Correction Principle explaining that nothing in the principle compels an organisation to refuse to provide an individual with access to his or her health information.

Proposal 38:

Guidelines be developed by the Privacy Commissioner that include detailed information about the process which should be followed to gain access to personal information, including guidance on requests for access, responses to those requests, how information is provided and fees.

Key stakeholder questions about UPP9 – Access and correction:
Q35. Do you agree with these proposals?

CSC Response

Yes.

Further, we strongly suggest that electronic means of access to records for review and correction be encouraged and even mentioned in the privacy principles. In the 21st century it should become unacceptable to continue with paper based approaches for individuals to access data about themselves.

Further, there should be no fees charged for individuals to correct data about themselves where the error/s was not their fault or creation.

Key stakeholder questions about UPP9 – Access and correction:
Q36. Are guidelines sufficient to ensure processes for access to health information are understood by agencies and organisations?

CSC Response

No. As Australia moves into the new paradigm of e-health, we believe a great deal of 'informative marketing' and education is required for the health sector to assist healthcare providers and their staff to understand what is acceptable and appropriate in terms of access to health records by individuals. These guidelines and education programs should include case studies and life-like examples and should be available in interactive formats.

Key stakeholder questions about UPP9 – Access and correction:
Q37. Are any other amendments to the access principle required?

CSC Response

As stated above, our recommendation is make a clearer indication that access is and should increasingly be by electronic and 'online' means.

Proposal 39:

The identifier principle should permit the use or disclosure of information that includes an identifier for funding, management, planning, monitoring, improvement or evaluation of health services and for research purposes in the public interest subject to the same limits that apply to health information being used or disclosed for those purposes.

Key stakeholder questions about UPP10 – Identifiers:
Q38. Do you agree with this proposal?

CSC Response

Yes

Key stakeholder questions about UPP10 – Identifiers:
Q39. Are any other situations where the identifier principle might have an inappropriate effect on the use or disclosure of health information?

CSC Response

Quite possibly. As stated above, in relation to health information, Australia is about to move into a new paradigm for healthcare using electronic health records. There needs to be capacity for the legislation and privacy framework to adapt over the next three to five years to evolution of the e-health agenda and changes in healthcare delivery making use of electronic records.

Proposal 40:

An agency or organisation should be allowed to use or disclose information outside Australia to lessen or prevent a serious risk to life, health, safety or welfare without continuing to be accountable for any misuse.

Key stakeholder questions about UPP11 – Transborder data flows:
Q40. Do you agree with this proposal?

CSC Response

Yes

Key stakeholder questions about UPP11 – Transborder data flows:
Q41. Are there any other exceptions for health information transferred outside Australia?

CSC Response

Quite possibly. As stated above, in relation to health information and the increase in international mobility and medical tourism, there needs to be capacity for the legislation and privacy framework to adapt over the next three to five years to evolution of the e-health agenda and changes in healthcare delivery making use of electronic records.

Section 2 - Our Submission – Further insights on health identifiers & privacy

In this section we offer some thoughts and examples from overseas that may assist AHMC, AHMAC, DOHA, NEHTA and others in consideration of health identifiers, electronic health records, privacy, consent and related issues.

CSC would welcome the opportunity to talk further about these areas in which we have expertise and experience.

Clarifying Privacy, Security, Consent & Credentialing

The advent of electronic health records and the expected new operating models for healthcare that may be enabled through electronic health records require greater clarity around the concepts of privacy, security, consent and credentialing.

Many Australians may appreciate receiving guidance from the government and their clinicians on what is reasonable to expect with respect to privacy of their health information, in particular guidance on what they should withhold or not withhold from their medical practitioners and other health providers. Also, medical practitioners may require guidance on sharing of information with their patients which may have traditionally been seen only by themselves.

Individuals and the medical community may require assistance in understanding privacy as opposed to security and their role in protecting the privacy of themselves and their patients and in engaging in appropriate security practices to support these protections.

Further, the issue of consent is often confused in this context. Within the context of electronic health records what consent/s are required by patients for the storage and/or sharing of their data?

Recent examples in the UK suggest some movement on this issue. Some National Health Service (NHS) Trusts have moved to complete electronic health records, no longer capturing or storing *any* data in paper format. If patients complain to this Trust that they do not wish their data to be stored electronically at all, the Trust in question has been reported as replying that they will be denied service and should seek service at another Trust. The Trust argued that it is not doing anything different with the data, it storing it in a different format but the core processes have not changed. Like all Trusts, this same Trust *is* obliged to ask for consent if they wish to share the patient data *outside* their Trust, but their position reflects that they are simply automating their current arrangements, not changing anything for which fresh consent is required.

Has Australia undertaken a privacy impact assessment in relation to health records? If not, we would propose that such an assessment should be undertaken. An assessment could then inform a privacy and consent strategy to support the program to implement national electronic health records.

Balancing privacy and usability and ease of access

As stated above, in several of our responses, privacy must be balanced with usability and ease of access. This is particularly important in the health sector in which health providers are often accessing or capturing data in an ‘urgent’ or ‘rushed’ situation. If privacy guidelines or related security restrictions

prove an impediment, we can expect a pragmatic health provider may, with good intentions, breach those guidelines in order to 'get their job done'.

We are working with health organisations in other countries to implement smart cards for health providers as an appropriately secure yet easy-to-use solution for electronic health records. Our work with smart cards has involved a great deal of testing to ensure the use of smart cards is easy and straightforward and 'response times' are reasonable for busy clinical staff. We are also currently working on trialling 'proximity cards' to provide even easier access for clinical staff (that is, as the staff person approaches a computer it recognises them). However current security policies in many jurisdictions do not adequately allow for new technology tools such as proximity cards and may require revision to ensure security remains robust and opportunities for privacy breaches are minimised.

Allowing individuals to control their own records

Surveys on digital trust and privacy indicate individuals are comfortable to divulge personal information if they have some control over the information and its dissemination, on an individual and personalised basis, as to what gets used, and if they have the chance to build up trust with organisations with whom they can be expected to share information. The process of building up and proving trust takes time.

To assist in building up trust, organisations and service providers, including hospitals and clinical staff, have to show integrity of word and deed – that is, that they do what they say they are going to do with the information and no more and they have to visibly adhere to privacy guidelines and security practices.

Giving individuals control over their own records greatly assists with supporting appropriate privacy principles. Perhaps even more important than 'control' is for individuals to have access to audit trails so that individuals can see who or what organisations have accessed their records and for what reasons.

Our work with the Netherlands implementing electronic health records through an index (see case study below) model includes functionality to allow individuals to see all access to their records.

Near-Future Trends for Healthcare Records

Legislative frameworks, policies and guidelines for health records need to accommodate the growing trends for new access methods for healthcare records and the increasing mobility of the population. Near future trends in access methods and data capture for healthcare records include:

- Biometric identification
- Genetic information linked with medical records
- International travel particularly in relation to medical tourism
- Text messages relating to medical appointments
- Telemedicine including virtual consultations, multiple clinicians
- Radio Frequency Identification Devices (RFIDs)
- Identity-as-a-service provided by independent not for profit organisations – this could evolve in response to the issue of governments having the dual roles of issuing and managing identifiers and related information and also policing and governing their use.

Regular review and assessment of legislative frameworks

As we outline above, e-health represents a new industry and the volume of activity in relation to online access to medical and health records is expected to grow exponentially. It would be unrealistic and naive to expect legislative frameworks to 'keep up' with all changes. We propose that the government anticipates and plans for regular reviews and revisions of the governing legislation. We propose three reviews of the legislative frameworks at least every three to four years.

Sample recent international media and research on related topics

Research - Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records, Management Science, Vol. 55, No.7, p. 1077-1093, July 2009

Researchers have found that states with restrictive privacy laws have decreased levels of electronic medical record (EMR) adoption. According to the article, states with laws that restrict hospitals from disclosing patient information have experienced an 11 percent decrease in EMR adoption over the past three years and a 24 percent decrease overall. States with no such regulations experienced a 21 percent gain in hospital EMR adoption. The effect is most evident in networks of hospitals and medical providers. In states without restrictive privacy laws, a hospital that adopts EMRs can spur others to adopt. When one hospital adopts EMRs, the probability of other hospitals in the community adopting EMRs rises by 7 percent. The authors of the article say that hospitals may be more likely to adopt EMRs if they can reassure patients that their confidentiality is legally protected. However, they warn that privacy protection may inhibit adoption if hospitals cannot benefit from easily exchanging patient information.

Access: Miller and Tucker, Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records, *Management Science,* Vol. 55, No.7, p. 1077-1093, July 2009 – abstract only – subscription or purchase required for full article.

Report: HITECH's Impact on Health Information Exchanges: Key Decision Points for Privacy and Security

Health Information Exchanges (HIEs) enable authorised caregivers, patients, public health authorities, and other providers to share electronic patient health information across different settings and geographical areas. With the ability to send and request health information, an authorized physician can access a patient's medical history and obtain a list of current medications, known allergies, and other vital information, regardless of where it was originally recorded. These powerful capabilities, however, must be made secure and confidential in order to win the trust and consent of patients. To address these areas, organizations need to: 1) determine which data to share and how to share them, 2) develop practices to manage authorized access, 3) adopt policies and practices to prevent unauthorized access, 4) gain consent from patients, and 5) be prepared to address breaches. This paper identifies key decision points related to HIE privacy and security and discusses the impact of relevant provisions and requirements contained in the HITECH Act. It also includes examples of best practices from HIEs in both the United States and Europe.

Access report: http://www.csc.com/health_services/insights/30034-hitech_s_impact_on_health_information_exchanges_key_decision_points_for_privacy_and_security

Article – Digital Health: Struggle or a Pipe Dream? *CNNMoney.com*, July 31, 2009, David Goldman
"Creating an electronic health record (EHR) for every American by 2014 is a big part of Obama's agenda, but it may be easier said than done."
That statement summarizes problems three delivery networks faced as they installed and implemented systems. In addition to cost, which was a challenge for each of them, the scale of workflow and other policies and procedures required and getting providers to adopt technology were major hurdles. Western Carolina Health Network, for example, spent four years just drafting legal agreements among its 16 hospitals to establish where patient records are located and by whom, how, and when they can be accessed. According to a representative of one of the IDNs, "Technology is the easy part; the hard part is working with independent providers"
Access article:
http://money.cnn.com/2009/07/31/news/economy/electronic_health_records/?postversion=2009073103

Research - Are Electronic Health Records Ready for Genomic? *Genetics in Medicine*, Vol. 11, Issue, 7, p. 510-17, July 2009
According to a recent study, electronic health records (EHRs) have the potential to enable clinical integration of genetic/genomic medicine into routine practice, but standardized data elements and additional EHR functionality will be needed. The researchers conducted semi-structured interviews with 56 participants – including medical geneticists, genetic counselors, primary care physicians, and EHR vendors and specialists – with the goal of determining the present and future role of EHRs in storing and using genetic information. Three-fourths of the healthcare providers interviewed reported that current EHR systems did not meet genomic/genetic medicine needs. The respondents cited problems with collection of family history, documentation, and organization of information, as well as a lack of demand for genetic content and privacy concerns as barriers to integration. Many stated that genetics/genomics would be a driver of content in the next five to ten years.
Full details of the study are available for purchase online. Access here: Study Finds Electronic Health Records Not Ready for Genetic Information, *Genetics in Medicine*, subscription or purchase required

Article – The Doctor will text you now. The Wall Street Journal, July 3, 2009

Online communication between patients and physicians ("digital medicine") was described in *The Wall Street Journal* on July 3 as a practice that is growing in response to increasing insurer coverage of care delivered in this way. "So far, the most common digital doctor services are the simplest ones, like paying bills, sending lab results, and scheduling appointments." But, as illustrated in the article, more patients are using the medium to ask about minor health issues and physicians are encouraging this practice as more insurers get on board. Aetna, Cigna, and Blue Cross Blue Shield plans in some states are all mentioned as currently reimbursing for e-visits. Humana and Wellpoint also have programs in some parts of the country. "Doctors who offer digital visits say they generally are most effective for treating mild, simple conditions, often when patients are too busy or too far away to come to the office. Ailments most frequently treated online include sinus problems, cold and flu symptoms, urinary infections, and coughs. Other common conditions are back pain and sleep issues." The article mentions several online services that support e-visits: RelayHealth, Medem, and American Well (which also supports Web video, live chat, or telephone communications) and includes several examples of satisfied patients and physicians.
Access: Anna Wilde Mathews, The Doctor Will Text You Now, *The Wall Street Journal*, July 3, 2009 (subscription required).

Article: Five trusts breach data protection law. UK Smart Healthcare, Wednesday 15 July 2009
Hospital trusts including Royal Free Hampstead, Chelsea and Westminster and Hampshire Partnership have been reprimanded by the ICO after failures to encrypt data

A total of five trusts, also including Surrey and Sussex, and Epsom and St Helier, have signed formal undertakings to process personal data legally in future, the Information Commissioner's Office said on 14 July 2009.
Royal Free Hampstead NHS Trust said it had lost an unencrypted CD containing data on 20,000 cardiology patients' medical treatment. Hampshire Partnership NHS Trust said an unencrypted laptop with data on 349 patients and 258 staff was stolen from an employee at a conference.
Similarly, Chelsea and Westminster Hospital Foundation Trust reported the loss of an unencrypted memory stick which was not even password protected, probably stolen from an unlocked office. A member of staff had been taking it home for use on his own computer.
The three trusts will in future encrypt and password protect laptops, mobiles and portable devices.
A ward handover sheet containing data on 23 patients in the care of Surrey and Sussex NHS Trust was found on a bus, and the trust also said it had lost two unencrypted laptops, although they were kept behind three locked doors. Meanwhile, Epsom and St Helier University Hospital NHS Foundation Trust stored hospital records insecurely for nearly two years.
All the five trusts have agreed to implement appropriate security measures and train staff on storage policies.
"These five cases serve as a reminder to all NHS organisations that sensitive patient information is not always being handled with adequate security," said Sally-Anne Poole, the ICO's head of enforcement and investigations. "It is important that staff adhere to policies designed to protect individuals' sensitive information."
Access: http://www.smarthealthcare.com/

Report - Liability Coverage for Regional Health Information Organizations, AHRQ National Resource Center for Health Information Technology, June 2009

“As the field of HIE continues to expand, questions surrounding liability have become a central concern to RHIOs and their partners.” These concerns are related to potential liability for negligence (in the protection of patient healthcare information) guaranteed by business associate agreements healthcare providers and other HIPAA-covered agencies are required to have with RHIOs. These concerns are also leading RHIOs to considering liability insurance.
According to a June 2009 AHRQ report, there are five key questions surrounding RHIO liability insurance:

- How do RHIOs distribute liability among partners?
- Which partnering entities currently take on liabilities? What are the liability concerns of RHIO partners?
- What levels of liability coverage are appropriate? What factors affect these levels of coverage?
- How do RHIOs find and manage brokers and underwriters?
- What are the impacts of law and government on a RHIO‟s liability?

The report reviews these questions and the actions of six operating RHIOs in the U.S. The conclusions include significant legal uncertainty regarding RHIO liability, what appear to be levels of liability that vary depending on data ownership and access (such as federated vs. decentralized data access), and difficulty finding insurers. Yearly premiums reported ranged from $18,000 to $55,000.

Access & Details: Prashila Dullabh, M.D. and Maria Molfino, B.A., Liability Coverage for Regional Health Information Organizations, AHRQ National Resource Center for Health Information Technology, June 2009

Article - The Tories' next privatisation GC Weekly (Guardian Mail) – 13 August 2009 (reproduced)

Last year, David Cameron wanted to get rid of a mythical NHS supercomputer, *writes SA Mathieson.* Now, the Conservative Party has published an independent review of NHS IT along with a series of sensible policies, marking a maturation of its approach.

The Tory plans can be criticised for closely following the Department of Health's more recent policies, such as moving control away from the centre and reworking some of the National Programme for IT's central deals. However, if something is an obvious thing to do, there is little sense in opposing it.
Some clear blue water opens up when it comes to Conservative plans to give patients greater control over their personal health records. This is stimulating a debate over privacy, particularly over whether an advertising led firm such as Google or Microsoft should host such records.
However, individual control of records - health and otherwise - has huge promise as a way to defuse some of the 'surveillance state' privacy rows of the last few years. The Conservatives, and others interested in placing government IT firmly on the citizen's side, need to work on how this new type of privatisation might work in practice.
Access: http://www.smarthealthcare.com/