Office of the Information Commissioner
Queensland

SUBMISSION TO AHMAC
Healthcare identifiers and privacy: Discussion paper on proposals for legislative support (July 2009)

The Queensland Office of the Information Commissioner is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government.

Under Queensland's new *Information Privacy Act 2009* the Office of the Information Commissioner has performance monitoring and support functions. These statutory functions include commenting on any issues relating to the administration of privacy in the public sector. This submission provides some general observations and then answers questions for both the Part A proposals and Part B proposals.

Attachment A to this submission also provides a summary of the Queensland privacy principles, so that you have a full knowledge of our legislation's privacy coverage.

General comments

Unique health identifiers have been identified as foundational to the national E-Health Strategy. The Queensland Information Commissioner supports the utilisation of technology to improve the safety and sustainability of the health system and recognises that this will bring changes to the way information is accessed and shared. The discussion paper recognises 'getting privacy right' as a critical dependency for the national E-Health Strategy which asserts consumers will have confidence information is managed securely and confidentially. There are a number of reasons consumers may feel sceptical about this claim:

- despite privacy being identified as a primary concern for public confidence in the system, AHMAC proposes to proceed with introducing health identifiers prior to ensuring adequate privacy protections are in place. The credit reporting scheme provides an ongoing example of privacy rights being eroded by commercial interests without effective risk mitigation measures. That system has demonstrated an ongoing inability in the face of repeated consumer criticism to create and maintain accurate records, fundamentally affecting a person's ability to obtain credit and stigmatising the person.

Article 12 of the Universal Declaration of Human Rights[1] states:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

AHMAC has a responsibility to ensure that everyone has the right to the protection of an adequate law against interference with a person's privacy. To proceed without identifying and dealing with privacy concerns sends a powerful message about the actual importance ascribed to privacy protection. A strong commitment to privacy in the establishment of E-Health may somewhat allay consumers concerns of a repeat of government permitting a powerful system to be established only to later find that they find the risk mitigation measures put in place are not rigorous enough to adequately deal with concerns or are not effectively implemented.

[1] UN GAOR (1948).

Such risk mitigation strategies should include provider access controlled by consumer consent and the limiting of personal details recorded for each patient record.

- AHMAC proposes to override existing IPPs/NPPs by legislating for the utilisation of personal information collected by Medicare for another purpose.

An implementation process that respects the existing privacy regulatory framework in each incremental step taken to establish E-health will instil greater public confidence in the system, recognises that compliance with that regulatory framework has real costs and provide leadership to the health system in core values including privacy protection, consumer participation, citizen centred service delivery and consumer choice.

The primary benefits associated with the reforms for administrators come from an improved ability to match and link data. It cannot be assumed that the general public will understand the new capabilities of the system or the potential of the system in relation to enforcement issues. It is therefore important that participation in the system by consumers is premised on them having a clear understanding of how their personal information will be used throughout the E-Health system; who controls, has access to and permits the use of unique health identifiers; and what the legislative parameters are. While E-Health may permit greater scrutiny of health services, E-Health will collect massive amounts of personal information which can be duplicated at the click of a button. The system must have the flexibility to allow consumers to receive health services anonymously or to restrict how their personal information will be used in the administration of the service and wider health system.

The proposal to override the IPPs/NPPs through legislation sends the message that while governments are prepared to expend billions in developing the system, they are not prepared to accommodate the cost of privacy.

- The discussion papers on E-Health and the unique health identifier appear unbalanced in that they emphasise the benefits of the proposals, do not highlight the fact that success depends on necessary concomitant reforms in workflow reform, compliance costs, a shift to patient centred service delivery models, and resourcing. For example, it is claimed E-Health will improve continuity of care. An element of continuity of care depends upon effective communication between hospitals and local treating practitioners. At the local level the current paper based system use patient names and dates of birth as the unique patient identifier. A common system failure is for hospitals not to provide discharge summaries to the local practitioner. As the relevant part of the health system already has a unique patient identifier, creating a unique number alone will do nothing to improve continuity of care. Replacing facsimile or letters with emails or other form of electronic communication also will not of itself improve continuity of care. Associated reforms in business rules, adequate training, resources to adequately maintain the E-Health system and fail safe measures need to be developed. Even then, improved performance may not be guaranteed. E-Health reforms should not occur at the expense of privacy in circumstances where the other necessary reforms are not included and funded in the project.

- The evidence cited for cost savings appears to overstate the case for savings. This undermines confidence in the reforms being evidence based and not

based on intuition or conventional wisdom. For example it is claimed that 18% of medical errors are due to inadequate availability of patient information and this accounts for 3% of total costs or $3 billion in avoidable annual expenditure. For E-Health system achieve $3 billion in savings depends upon two pre-conditions:

- such errors are not attributable to medical intervention at times of emergency, professional competency in history taking, nor failure to read, make or obtain available records
- a consumer's full medical history will be ubiquitously and fully available through the national health system to health practitioners without consumer consent

The fundamental human right to privacy should not be eroded without an adequate evidence base and an equally energetic reform agenda in relation to the other necessary concomitant reforms.

Part A: National Healthcare Identifiers and Regulatory Support Proposals

The primary concern with moving forward in the way contemplated in the discussion paper—introducing the Healthcare Identifier Service (**HI Service**) and supporting systems and framework under the fragmented and unequal privacy protections present across Australia[2]—is that the protection for, and rights of, individuals should their personal information be misused, mismanaged, or improperly used or disclosed will not be equal. The discussion paper notes "Australian's [sic] expect their health information to be secure and used appropriately[3]", and "[if] consumers and providers are to actively participate in e-health systems, including the HI Service, there must be a high level of trust and confidence in their operation". All Australians, and some non-Australians, will be required to have a healthcare identifier, yet—depending on the jurisdiction in which they live or receive healthcare services—they will not have access to the same level of protection for personal information associated with that identifier. This is of significant concern, particularly as the proposals involve the introduction of a single identifier for each individual to be used across all public and private healthcare providers.

Given the short timeframes mentioned in the discussion paper for the introduction of the Uniform Privacy Principles (**UPPs**)[4], it would seem appropriate to consider introducing the HI System only after the national consistency has been achieved. This would ensure all Australians would have access to equal levels of privacy protection for their personal information forming part of or linked to the HI System.

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

An issue of concern about the powers being conferred on the Medicare CEO is the apparent lack of any powers in relation to taking and dealing with complaints, particularly from individuals, about the healthcare identifiers. While it is possible that Medicare's existing complaint handling powers may extend to the healthcare identifiers, it would be far more certain, and far more robust, for explicit and specific complaint handling powers to be built into the proposed legislative amendments to address this issue.

[2] Discussion paper, page 3.
[3] Discussion paper, page 12, section 2.3.1.
[4] Discussion paper, page 42.

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?

There are significant issues raised by this proposal, and these issues are identified in the discussion paper at page 3, which sets out the consequences of Australia's "patchwork of inconsistent and overlapping [privacy] requirements". The preamble to proposal 2, to which this question relates, states that the way in which personal and health information is collected, used or disclosed is regulated by privacy laws that have been put in place by Commonwealth, state and territory governments. Legislation of this kind is not present in every jurisdiction, as is set out in Part B, Table 1. The result of relying on the existing framework is highly likely to be inconsistent and fragmented protection of healthcare identifiers and associated personal information. This is of significant concern because, as the discussion paper notes, "[if] patients lack confidence around privacy protection they may not seek treatment or may withhold information, resulting in harm to themselves or others[5]".

This fragmented protection could be bolstered through the introduction of a regulatory framework to support the proposed healthcare identifiers, if the framework included specific provisions regulating permitted uses and disclosures and associated offence provisions. If the healthcare identifier itself is protected and regulated, in a way similar to the regulation applying to tax file numbers, the risks associated with relying on Australia's privacy patchwork could be reduced. This would also have the likely consequence of increasing public confidence in the new healthcare identifier, a factor identified at section 2.3.1 of the discussion paper as imperative for its success.

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?

It is likely that there will be circumstances where penalties for misuse would not be sufficient, e.g. where an individual suffers an identifiable harm as a result of the misuse of a healthcare identifier or associated information. If the misuse occurs in a jurisdiction where there is no provision for compensation as a result of such a misuse, individuals could be fundamentally disadvantaged because of the jurisdiction in which they live. It would be appropriate to consider including redress options for individuals in these circumstances, to ensure that all Australians have access to the same rights where their healthcare identifier or associated information is misused.

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

Use of the current definitions in enabling legislation should be appropriate. Any variation between jurisdictions should be acknowledged in the drafting process, and definitions drafted so as to overcome any such differences.

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

There are several terms mentioned in the discussion paper which do not have immediately identifiable meanings, for example *legitimate purpose* and *administering*

[5] Discussion paper, B.1.1.1, page 44.

the identifiers function. If these are intended to appear in the enabling legislation, they will require definition.

Additionally, where terms are used that may have different meanings across Australia's various jurisdictions, it will be important to define these so that there is no confusion about what is intended. No assumptions should be made as to the existence of a common definition across public and private healthcare providers and individual users.

There is already a general lack of awareness amongst consumers as to the extent of data use within the health system. There is always the potential for new data matching and data linking that may have the effect of eroding a person's right to privacy. For these reasons general catchall terms should be avoided and the purpose and use data is collected should be defined more specifically than 'for administrative purposes' or for what the consumer might 'reasonably expect'.

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

The proposed limits appear to provide personal information protection to a certain extent however, unless they are supported by effectively implemented compliance provisions, they are unlikely to be adequate.

A secondary issue, not canvassed by the question but raised within the information preceding it, is the issue of whether or not an individual will be able to receive a healthcare service without the use of a healthcare identifier. It is stated on page 18 that an individual will not be required to provide their healthcare identifier in order to receive a healthcare service, which creates the impression that the healthcare identifier is not required for provision of a healthcare service. However, A.5.2.4 sets out that the healthcare identifier database may be searched by healthcare providers on a number of demographic details. This indicates that, if an individual does not supply their healthcare identifier then the healthcare provider will acquire from the HI Service.

This point needs to be clarified, and if it is proposed that the provision of healthcare services must involve the healthcare identifier, retrieved by the provider if not supplied by the individual, this needs to be made explicitly clear.

It is most important that the compulsory aspects of the linked up system do not dissuade any individual from seeking medical advice. Consumers have a right to receive health care anonymously, and the E-Health system should allow consumers to do so. It should also allow consumers the option of limiting the use of their personal information including use only by the immediate health service for administrative purposes. The present approach does not make it clear to consumers that they will still receive a health service even if they do not give full consent to all proposed uses of their personal information. Consumer consent forms should be required to point this out to consumers.

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

Such an authorisation is required. Generally, the privacy principles relating to secondary use or disclosure based on reasonable expectation require the individual

to have held that reasonable expectation at the time the personal information was collected. It is unlikely that an individual could be said to have reasonably expected that their personal information would be used or disclosed as part of a healthcare identifier system when such a system was introduced after the information collection occurred. Given the complexity of the system and the proposed new ways of accessing and using informing, specificity in the nature of any secondary use is desirable except where what is proposed replicates existing implied consent practices. For example, a GP advises a patient specialist advice is desirable and obtains the consumer's consent to refer the consumer to a specialist, either expressly or impliedly. The transmission of required personal information can occur under existing arrangements with the use of the unique health identifier. However where new matching and linking of data is to occur with the use of the unique health identifier, this should be explicitly drawn to the consumers attention so that they are aware and can give informed consent as to the secondary use of the data.

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

Please see comments above at question 6.

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?

The penalties mentioned in the discussion paper are limited to unauthorised disclosures. Unauthorised or non-permitted disclosure is not the only threat to the privacy of individual's health information. It would be appropriate that these provisions extend to unauthorised use, access, modification and any other misuse, and to loss of information.

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?

It would be appropriate that offence provisions be accompanied by suitable penalty provisions.

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

Given that there is a lack of consistency across Australian jurisdictions, as mentioned above at question 2, including certain jurisdictions that lack applicable legislation and rely only on administrative arrangements, it is difficult to say that the existing arrangements will provide sufficient secondary use requirements for organisations.

However, there is general consistency in the fundamental approach to permitted uses across jurisdictions which have applicable legislation, e.g. exceptions where an individual has agreed, where the use is necessary to prevent threats to life or health, or for law enforcement purposes. These commonalities could form the basis of permitted uses in the enabling legislation, which would allow the healthcare identifier to be consistently protected, assist in overcoming the fragmented protection provided by Australia's patchwork privacy laws, and avoid the introduction of inconsistency.

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

Please see comments above at question 2.

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

Please see comments above at question 2.

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

Please see comments above at question 2.

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

While access and correction capabilities for individuals can be met by existing right to information or freedom of information laws, which are sufficiently similar across Australian jurisdictions in the rights they provide for individuals to access and correct their personal information, these laws apply only to government. Where healthcare identifiers and related information will be held by private sector healthcare providers, there may be circumstances where they are not covered by legislation which provides a right of access and correction.

The proposal to introduce a unique health identifier will create increased workload for regulators. The proposal cannot be seen in isolation from the broader E-Health system. Risks of such a system include that privacy breaches will occur more readily; be less detectable externally to agencies and the scale of a privacy breach will increase dramatically because of the massive amount of data that will accumulate, be matched and linked. Regulators will require increased resources for any increase in demand as a result of the implementation of E-Health and they will require forensic electronic investigation capacity and powers that presently do not exist.

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

Please see comments above at question 2.

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

Contrary to what is stated in A.5.2.11, Queensland is a state where the transborder data flow laws apply only to the transfer of personal information outside of Australia[6].

[6] Section 33, *Information Privacy Act 2009* (Qld).

Transfer within Australia attracts no special rules or considerations over and above transfer within Queensland.

However, with regard to states and territories where transfer within Australia is regulated, it is likely that the implementation of the proposed HI Service, and exchange of healthcare identifiers and associated information between healthcare providers, the trusted data source and the HI Service, could be hindered by existing transborder data flow rules.

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

See above at question 19.

Part B: Proposed National Privacy Reforms

In general, the Australian Law Reform Council's (**ALRC**) approach regarding health information is preferred. The UPPs are intended to be of universal application across all aspects of the public and private sectors. In order for this to be achieved, they must be as broadly applicable as possible. Health information—which is only relevant to certain organisations—requires different protections, as recognised by the ALRC in their recommendation that the UPPs be supported and modified by health specific regulations applicable to the healthcare sector and other organisations which deal with health information.

If the UPPs are redesigned to address the specific requirements of health information, rather than having those requirements in a separate regulation relevant only to those involved with health information, unnecessary burdens could be placed on organisations for which health information is not a factor. Additionally, where a health information specific regulation is used, it could be amended with reference only to the relevant organisations; with UPPs redesigned to cover health information, those health specific changes would require the input of all sectors, with the potential to cause unnecessary delay.

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

The suggested requirements would add robustness to the move towards national unification; however it is more appropriate that issues relating to guidelines and standards—publications which provide support and guidance in the implementation and application of privacy legislation—are addressed in joint policies or agreements between the jurisdictions, rather than in the legislation.

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

As noted above at question 24, issues relating to guidelines and standards are more appropriately dealt with through joint policies and agreements.

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

Whichever approach is taken in the UPPs towards the applicability of privacy legislation to information about the deceased, there would appear to be little value in drawing a distinction between health information and other information.

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

The proposed definition of health service provider would be more appropriate if a 'health service' was also defined in the legislation, in a non-exhaustive way. It would provide guidance to those using the legislation and clarify to what and to whom the health specific rules applied.

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

See above at question 26.

Should you require further information regarding the content of this submission please do not hesitate to contact my office on 07 3005 7155 or via email administration@oic.qld.gov.au.

Yours sincerely

Julie Kinross
Information Commissioner