Healthcare identifiers and consumer privacy protection:

submission to the Senate Community Affairs Legislation Committee's Inquiry into Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010

9 March 2010

Robin Banks, Chief Executive Officer

Level 9, 299 Elizabeth Street, Sydney NSW 2000 • DX 643 Sydney
Phone: 61 2 8898 6500 • Fax: 61 2 8898 6555 • www.piac.asn.au

Contents

Introduction

The Public Interest Advocacy Centre

The Public Interest Advocacy Centre (PIAC) is an independent, non-profit law and policy organisation that works for a fair, just and democratic society, empowering citizens, consumers and communities by taking strategic action on public interest issues.

PIAC identifies public interest issues and, where possible and appropriate, works co-operatively with other organisations to advocate for individuals and groups affected. PIAC seeks to:

- expose and redress unjust or unsafe practices, deficient laws or policies;
- promote accountable, transparent and responsive government;
- encourage, influence and inform public debate on issues affecting legal and democratic rights;
- promote the development of law that reflects the public interest;
- develop and assist community organisations with a public interest focus to pursue the interests of the communities they represent;
- develop models to respond to unmet legal need; and
- maintain an effective and sustainable organisation.

Established in July 1982 as an initiative of the (then) Law Foundation of New South Wales, with support from the NSW Legal Aid Commission, PIAC was the first, and remains the only broadly based public interest legal centre in Australia. Financial support for PIAC comes primarily from the NSW Public Purpose Fund and the Commonwealth and State Community Legal Services Program. PIAC also receives funding from the Industry and Investment NSW for its work on utilities, and from Allens Arthur Robinson for its Indigenous Justice Program. PIAC also generates income from project and case grants, seminars, consultancy fees, donations and recovery of costs in legal actions.

PIAC's expertise in privacy, health and human rights

PIAC has a long history of interest in, and concern about, the appropriate protection of privacy rights within both the public and private sectors. PIAC has been a strong advocate for the protection of the privacy rights of Australians, particularly the rights of individual Australians to control their personal information and to be free of excessive intrusions. PIAC's work as a consumer advocacy organisation, particularly in relation to health matters, has required PIAC to consider privacy issues because they are frequently a matter of concern to many people who contact the Centre.

Specifically in relation to the development of electronic health records and healthcare identifiers, PIAC has been involved in the consultations conducted by National E-Health Transition Authority (NEHTA) and the

Department of Health and Ageing (DoHA) and made a submission to DoHA in January 2010 in response to the Exposure Draft Healthcare Identifiers Bill 2010 (the Exposure Draft Bill).[1]

In recent years, PIAC has provided legal advice and assistance to clients in a number of matters involving alleged breaches of the *Privacy and Personal Information Protection Act 1998* (NSW) (the PPIP Act) and the *Privacy Act 1988* (Cth) (the Privacy Act). In 2006, PIAC represented the respondent in *Director General, NSW Department of Education and Training v MT* [2006] NSWCA 270, a landmark case concerning the interpretation of several key provisions of the PPIP Act. In another matter before the Office of the Privacy Commissioner (OPC) PIAC represented a former Villawood detainee whose personal information was inappropriately disclosed to the media.

PIAC has played a leading role in privacy debates in Australia in recent years, contributing to a number of inquiries and reviews at the national and state level. Recent submissions by PIAC have addressed the privacy implications of the proposed Health and Social Services Access Card[2], and the proposal by the Australian Bureau of Statistics to implement a longitudinal study in the population census (a proposal requiring capacity to data match over time).[3] In October 2007, PIAC made a submission to the first Consultation Paper in the current reference from the New South Wales Law Reform Commission (NSW LRC), *Consultation Paper 1 – Invasion of Privacy*.[4] In December 2007, PIAC made a submission in response to *DP72: Review of Australian Privacy Law*, as part of the reference on privacy being conducted by the Australian Law Reform Commission (ALRC). PIAC also participated in the consultations conducted by and made submissions to the Federal Department of the Prime Minister and Cabinet in relation to amendments to the Privacy Act in relation to the establishment of Unified Privacy Principles and amendments in relation to health information privacy.

PIAC Chief Executive Officer, Robin Banks, is a member of the Privacy Advisory Committee (PAC), which provides strategic advice to the Federal Privacy Commissioner on privacy issues and the protection of personal information.

PIAC has also undertaken a considerable amount of work on patient or health care rights over its 26 years of operation, in particular around patient safety, complaints and investigations processes, health privacy and the development of an Australian Health Consumers' Charter.

---

1 Robin Banks, *Not yet ready for exposure: response to the Exposure Draft Healthcare Identifiers Bill 2010* (2010) Public Interest Advocacy Centre <http://www.piac.asn.au/publications/pubs/sub2010011_20100115.html> at 4 March 2010.

2 Public Interest Advocacy Centre, *Health and Social Services Access Card: Submission to Access Card Consumer and Privacy Taskforce, Discussion Paper* (2006); Public Interest Advocacy Centre, *Access Card Proposal Still Fails Public Interest Test: Comment on the Exposure Drafts of the Access Card Legislation* (2007).

3 Public Interest Advocacy Centre, *Submission to the Australian Bureau of Statistics on Enhancing the Population Census: Developing a Longitudinal View* (2005).

4 Public Interest Advocacy Centre, *Matching Rights with Remedies: a statutory cause of action for invasion of privacy, Submission to the NSW Law Reform Commission on Consultation Paper 1 – Invasion of Privacy* (2007).

PIAC welcomed the endorsement of the Australian Charter of Healthcare Rights by the Australian Health Ministers in July 2008. PIAC participated in the consultation process that led to the Commission's draft charter, including providing a written submission in response to the Consultation Paper on the draft charter.

PIAC also made a submission to the Senate Select Committee on Medicare in 2003.

PIAC has a long-standing interest and expertise in the scope and application of international human rights, including the right to privacy. It has conducted a national 'Protecting Human Rights in Australia' project since 2004 and has made numerous submissions to government and other inquiries in relation to issues that have the potential to interfere with human rights.

The current inquiry and this submission

PIAC welcomes the opportunity to provide this submission to the Senate Community Affairs Legislation Committee (the Committee) in response to the Committee's Inquiry into the Healthcare Identifiers Bill 2010 and the Healthcare Identifiers (Consequential Amendments) Bill 2010 (the Inquiry). In this submission, PIAC provides brief introductory comments on the context of the Healthcare Identifiers Bill 2010 (the Bill) and the Healthcare Identifiers (Consequential Amendments) Bill 2010 (the Amendment Bill) (together, the Bills) and then provides detailed comments in relation to the content of the Bills.

The Healthcare Identifiers Service

PIAC has previously provided critical comment on the approach being taken by the Federal Department of Health and Ageing to the development of healthcare identifiers and the Healthcare Identifiers Service, being the name given to the system for implementation of a system of allocating and using unique healthcare identifiers as part of the development of a national electronic health records system. While the drafting of the Bill reflects some amendments to the Exposure Draft Healthcare Identifiers Bill 2010 (the Exposure Draft Bill) that respond to concerns raised by PIAC and other consumer advocates, there remain some elements of the Bill that result in the proposed Healthcare Identifiers Service being unclear, insufficiently regulated and having inadequate privacy protections.

PIAC is of the view that it is vital that the potential benefits of electronic health records be realised without increasing the risk to consumers of the privacy of their sensitive personal information being compromised. Any such increase in risk has the potential to seriously undermine consumer confidence in electronic health records and their trust in healthcare providers and government.

General comments

The right to privacy and healthcare rights

A key focus in the development of the healthcare identifiers system should be on ensuring proper protection of the healthcare consumers' individual right to privacy. The right to privacy is a fundamental human right that has been recognised as such in key international instruments including the *Universal*

Declaration of Human Rights[5] and the *International Covenant on Civil and Political Rights* (ICCPR).[6] Australia is a State Party to the ICCPR and, as such, is obliged to ensure the protection, promotion and fulfilment of the right to privacy.

PIAC also notes that the Australian Health Ministers, in endorsing the Australian Charter of Healthcare Rights, have recognised the right to privacy of healthcare consumers.[7]

While PIAC recognises that privacy is not an absolute right and that it must be balanced against other rights (such as freedom of expression), PIAC is concerned that the Bill fails to properly recognise and protect the right and adequately deal with infringements of the right.

The current context

PIAC is concerned that there are two significant Federal Government processes taking place in relation to healthcare and privacy and they do not appear to be working in concert. The two processes are the development of the Healthcare Identifiers Service and the review and amendment of the *Privacy Act 1988* (Cth) (the Privacy Act) in respect of health information.

PIAC urges the Committee to recommend to the Federal Parliament and Government that the two processes are brought together and nothing further be done in respect of progressing the establishment of the Healthcare Identifiers Service until the amendments to the Privacy Act in respect of health information have been finalised. At that point it will become much clearer what, if any, further privacy protections will be necessary to ensure the proper protection of the right to privacy of healthcare consumers.

Recommendation

1. *That the Senate Community Affairs Legislation Committee recommend to the Parliament that debate and voting on the Healthcare Identifiers Bill 2010 (Cth) and the Healthcare Identifiers (Consequential Amendments) Bill 2010 (Cth) be postponed until the amendments to the* Privacy Act 1988 *(Cth) in respect of health information privacy are enacted.*

Legislative purpose

The Explanatory Memorandum to the Bills: indicates that the:

> … purpose of the Healthcare Identifiers Bill 2010 … is to implement a national system for consistently identifying consumers and healthcare providers and to set out clear purposes for which healthcare identifiers can be used.[8]

---

5 *Universal Declaration of Human Rights*, GA Res 217A(III), UN Doc A/Res/810 (1948), Art 12.

6 *International Covenant on Civil and Political Rights*, 16 December 1966 [1980] ATS 23, (entered into force generally on 23 March 1976), Art 17.

7 *Australian Charter of Healthcare Rights* (2009) Australian Commission on Safety and Quality in Health Care <http://www.health.gov.au/internet/safety/publishing.nsf/Content/PriorityProgram-01> at 4 March 2010.

8 Explanatory Memorandum, Healthcare Identifiers Bill 2010 (Cth) and Healthcare Identifiers (Consequential Amendments) Bill 2010 (Cth) 2.

This fails, however, to identify what is the public good to be achieved through the establishment of such a Healthcare Identifiers Service. The Explanatory Memorandum goes on state that:

> Communication of health information is a vital part of effective healthcare. The accurate identification of individuals is critical in all health communication…
>
> Using an individual healthcare identifier will provide a way for healthcare providers to more accurately match the right records to the person they are treating and improve accuracy when communicating information with other healthcare providers.[9]

PIAC understands this to mean that the purpose is to facilitate appropriate transfer of healthcare information to improve healthcare outcomes. This purpose is commendable.

PIAC is, however, concerned that the actual Bill seems to contemplate broader uses for healthcare identifiers, including 'the management (including the investigation or resolution of complaints), funding, monitoring or evaluation of healthcare'[10], the 'provision of indemnity cover for a healthcare provider'[11] and the 'conduct of research …'[12]

All of these purposes significantly change the context and scope of the Healthcare Identifiers Service and raise, for PIAC, concerns about the Federal Government's overall purpose in respect of healthcare identifiers. PIAC has previously made extensive submissions about the privacy risks of the former Federal Government's proposed healthcare card, concerns that seemed to be understood and shared by the current Government when in opposition. Yet, the inclusion of 'management …, funding, monitoring and evaluation of healthcare' as a purpose for which healthcare identifiers are authorised to be used and/or disclosed, suggests that the identifiers could replace Medicare numbers and cards for the purpose of management and funding of the provision healthcare services.

Further, the additional purposes authorised under clause 24(1)(a)(ii) and (iv) are inconsistent with the use of de-identified data in research. It is not at all clear from the Bill or supporting documentation why the use of healthcare identifiers is necessary or desirable in respect of either of these purposes. Indeed, sound research generally relies on de-identified data to protect the integrity of the research.

PIAC considers that the inclusion of such authorised use and disclosure in clause 24 is a clear example of function creep, where provisions and mechanisms designed specifically for one purpose over time expand to permit other activities. Function creep was identified by PIAC and others in respect of the healthcare card and appears to already be a serious risk of the Healthcare Identifier Service as it is developing.

---

9 Ibid.

10 Healthcare Identifiers Bill 2010 (Cth) cl 24(1)(a)(ii).

11 Healthcare Identifiers Bill 2010 (Cth) cl 24(1)(a)(iii).

12 Healthcare Identifiers Bill 2010 (Cth) cl 24(1)(a)(iv).

Recommendation

2. That the Healthcare Identifiers Bill 2010 (Cth) be amended to remove clauses 24(1)(a)(ii), (iii) and (iv).

Consumer rights

PIAC is pleased to see that Bill—as compared to the Exposure Draft Bill—now includes two clauses that provide for the disclosure of a healthcare recipient's healthcare identifier to that recipient.

Clause 18 mandates that the service operator:

> … must, if asked to do so by a healthcare recipient …, disclose to the healthcare recipient … the healthcare recipient's healthcare identifier … or the information that relates to the healthcare recipient or to the healthcare recipient's healthcare identifier …

Clause 25 allows a healthcare provider to disclose a healthcare recipients healthcare identifier to that recipient or a person who is responsible for that recipient.

PIAC believes that clause 25 should be redrafted to reflect the obligation in clause 18 as the current drafting is permissive of disclosure rather than mandating such disclosure if the healthcare recipient requests it.

Further, there is nothing that reflects Information Privacy Principle 7, which obliges government record keepers to, on request from the person who is the subject of record, make:

> … appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:(a) is accurate; and (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.[13]

The absence in the Bill of a clear statement of the right of the healthcare recipient to not only access but to seek correction of the information held by the service operator is extraordinary given the range of provisions that permit collection, use and disclosure of the healthcare identifier and identifying information of the healthcare recipient.

PIAC notes that the Bill has been improved by the addition in clause 10(b) of an obligation on the service operator to keep a record of 'details of requests made to the service operator for the service operator to disclose … healthcare identifiers'. This reflects PIAC's submission on the Exposure Draft Bill. PIAC is keen, however, for the Bill to provide greater clarity on this matter through the inclusion of a requirement that these records include:

- requests made for disclosure, whether or not there was a disclosure made and, if so, to whom;
- requests made for access by healthcare recipients or responsible persons under clause 18 and whether or not access was granted; and

[13] *Privacy Act 1988* (Cth) s 14.

- requests made by healthcare recipients to the service operator for correction of information held by it and whether or not correction was made.

Further, there is nothing in the Bill that requires data sources to keep a record of what information (including identifying information as defined in clause 7) has been disclosed to the service operator or the service operator to keep a record of what data sources provided information (including identifying information). Again, this absence needs to be rectified to ensure consumers have access to this information.

PIAC is concerned that all of the disclosures and uses of healthcare recipient identifying information and healthcare identifiers authorised under the Bill are without any requirement to obtain the consent of the healthcare recipient. Further consideration needs to be given to whether some or all of the disclosures and uses both of identifying information and of healthcare identifiers could and should require the consent of the individual consumer.

PIAC commends the Government on making it clear in the Bill—as compared to the Exposure Draft Bill—that a healthcare recipient can have knowledge of their healthcare identifier.

Recommendations

3. *That the Healthcare Identifiers Bill 2010 (Cth) be amended to provide healthcare recipients with the right to require the service operator to correct or annotate their healthcare identifier data held by the service operator from the date of system implementation.*
4. *That the Healthcare Identifiers Bill 2010 (Cth) be amended to require data sources, healthcare providers, entities and the service operator to keep a record of all disclosures and collection and use of information and healthcare identifiers and of all requests from healthcare recipients for access, correction or annotation and the action taken on such requests.*
5. *That the Healthcare Identifiers Bill 2010 (Cth) be amended to require data sources, healthcare providers and entities to provide a timely written report to the service operator of all disclosure and collection and use of information and healthcare identifiers.*
6. *That the Committee consider whether or not some or all uses and disclosures, other than to the healthcare recipient, of identifying information and/or healthcare identifiers of that healthcare recipient require individual consent.*

Lack of certainty and delegation of significant power to regulations

PIAC remains concerned about the number of aspects of the proposed Health Identifier Service that are dealt with in the Bill through empowering regulations to be made. Provisions operating in this way include the following:

- Clauses 6(2) and 12(2) – Definitions in respect of 'service operator' and 'data source'. This effectively permits new service operators, either public or private, to be introduced through regulation rather than being subject to the full scrutiny of the legislature, and for the data used by the service operator for 'purposes of the service operator assigning a healthcare identifier' to be sourced from currently unknown and unidentified sources again without the full scrutiny of the appropriateness of such

sourcing by the legislature. This means that potential future service operators and data sources permitted through regulation could be private sources.

- Clause 7 – the scope of information that can be included within the definition of 'identifying information' for the purposes of healthcare providers, whether individuals or otherwise, and healthcare recipients can be broadened through regulation. This means that such an expansion would not be subject to the same level of parliamentary scrutiny.

- Clause 9(5) – requirements for assignment of healthcare identifiers. Central to the proper protection of personal information in a scheme of this sort are clear and mandatory requirements for operation of the scheme. Yet, the Bill provides that 'regulations may prescribe requirements for assigning a healthcare identifier'.[14] Such a core element of the Health Identifier Service should properly be clear on the face of the primary legislation and should be dealt with at the time the Healthcare Identifier Service is established not at some later time. Under the Bill it would be possible for the Healthcare Identifier Service to be implemented and operational without any requirements prescribed in respect of the assignment of healthcare identifiers.

- Clause 14 – information to be provided to the service operator by healthcare providers. This clause enables information specified in as-yet-unmade regulations to be required of healthcare providers by the service operator.

- Clause 21 – access controls. This clause allows a matter that should be central to the legislative scheme to be left to regulation. It provides that regulations 'may provide rules about the disclosure of healthcare identifiers to the service operator, including rules about requests to the service operator to disclose healthcare identifiers'. Rules about disclosure and requests for disclosure go to the heart of the Healthcare Identifier Scheme and should be set out clearly within the enabling legislation.

- Clause 27 – protection of healthcare identifiers. Where an entity 'holds' healthcare identifiers, it is required to protect them against 'misuse and loss' (clause 27(a)(i)), unauthorised access, modification or disclosure (clause 27(a)(ii)), and to 'comply with any requirements prescribed by the regulations' (clause 27(b)). Clause 39(2) provides that a penalty for failure to comply with the regulatory requirements may be provided for in regulation. The clear statement of both obligations on entities that hold healthcare identifiers should be detailed in the enabling legislation as should the penalty for breach of both the statutory obligations set out in clauses 27(a)(1) and (ii) and any other obligations whether set out in regulations under clause 27(b) or otherwise.

In addition to these explicit provisions referring core matters to subordinate legislation, the broader regulation-making power contained in clause 39 of the Bill permits regulations to be made prescribing matters 'necessary or convenient to be prescribed for carrying out or giving effect to this Act'. This is an extraordinarily permissive provision.

---

[14] Healthcare Identifiers Bill 2010 (Cth) cl 9(5).

The reliance in the Bill on referral to regulation of such core aspects of the Healthcare Identifiers Service strongly indicates that the Bill is premature, with significant further work required to ensure proper consideration has been given to governance aspects and the scope of the Healthcare Identifiers Service.

Recommendation

7. *That the Healthcare Identifiers Bill 2010 (Cth) be amended to remove the reference of matters to regulation in clauses 6(2), 7, 9(5), 12(2), 14, 21 and 27 and replace them with express clauses dealing with the matters that are currently to be separately regulated.*

Absence of the consumer in establishment of healthcare identifier

Despite previous submissions on this matter, there remains nothing in the Bill that contemplates the healthcare recipient providing identifying information to permit the establishment of their healthcare identifier.

If the Health Identifiers Service is designed to improve healthcare through the better flow of information about healthcare, excluding healthcare recipients from applying for and providing identifying information seems extraordinary. It also seems to enable the whole Healthcare Identifiers Service to be established without the knowledge of healthcare recipients. This is an extremely poor public policy approach particularly in light of the previous strong concerns held by consumers about the establishment of national identifier systems.

Recommendations

8. *That the Healthcare Identifiers Bill 2010 (Cth) be amended to expressly permit healthcare recipients to request the allocation of a healthcare identifier and to provide identifying information to the service operator for that purpose.*
9. *That the Senate Community Affairs Legislation Committee recommend that the Government give urgent priority to informing the broader community of the proposed development and implementation of the Healthcare Identifiers Service and its key components and develop a community awareness strategy to be implemented at the time of the implementation of the Healthcare Identifiers Service to ensure healthcare recipients are aware of the Service and their rights in respect of the Service.*

Lack of express security obligations

PIAC notes that clause 27 requires 'an entity' to protect healthcare identifiers and clause 15 imposes a duty of confidentiality on 'persons', but remains concerned that there is nothing in the Bill that expressly deals with obligations on either the service operator or healthcare providers in receipt of healthcare recipient healthcare identifiers to have in place strong information security measures to protect those identifiers and/or any identifying information. The definition of entity in clause 5 of the Bill does not appear to capture the service operator although it may capture healthcare providers.

The wording of this clause—'An entity must take reasonable steps to protect …'—is not as strong as would be hoped for. PIAC submits that it would be better to place the onus on entities and the service operator in the following terms:

> The service operator must protect healthcare identifiers and identifying information that the service operator holds from …
> An entity, including a healthcare provider, must protect healthcare identifiers and identifying information that the entity holds from …

Further, as noted above, there is no penalty for a failure to properly ensure the security of healthcare identifiers and/or identifying information.

This is a gap that must be rectified before enactment.

Recommendation

10. That the Healthcare Identifiers Bill 2010 (Cth) be amended to include:

(a) specific obligations on the service operator and entities, expressly including healthcare providers, in possession of identifying information and/or healthcare identifiers to implement and maintain strong information security measures; and

(b) penalties for failure to ensure the security of healthcare identifiers and identifying information.

Comments on specific provisions of the Bill

'Identifying information': clause 7

PIAC urges the Committee to consider recommending for the reduction the scope of 'identifying information' within the definition in clause 7 that is permitted to be disclosed by a data source and/or collected by the service operator for the establishment of a healthcare identifier. For example, it is not clear how collecting information on the birth order of a person who is a twin or triplet would be necessary to identify the person, as it is highly unlikely that more than one of the children within a multiple birth would have the same name.

The purpose of collection

Clauses 11(2), 13(2), 16(2), 20(2) and 24(2) of the Bill are all drafted in such a way as to technically permit collection of information and/or healthcare identifiers for any purpose as the purpose aspect of these subclauses is included in paragraph (b) of each, which relates only to 'use' on the current drafting.

For example, clause 11(2) currently reads:

> The service operator is authorised:
> (a) to collect the information; and
> (b) to use the information for the purpose of assigning a healthcare identifier to the healthcare recipient.

As can be seen from this example, there is no purpose specified in respect of the collection of information in paragraph (a) while use of information is limited by the purpose included in paragraph (b).

These clauses should all be reworded to separate out the purpose limitation so that it applies to both paragraphs. So, in respect of clause 11(2) for example it would be amended to read:

> The service operator is authorised:
> (a) to collect the information; and
> (b) to use the information;
> for the purpose of assigning a healthcare identifier to the healthcare recipient.

While this appears to be a drafting error, it was identified in PIAC's submission on the Exposure Draft Bill and has not been corrected.

Recommendations

11. *That the words '… information for the purpose …' in subclause (b) of clauses 11(2), 13(2), 16(2) of the Healthcare Identifiers Bill 2010 (Cth) be amended to read:*

    '(b) … information;
    for the purpose …'

12. *That the words '… healthcare identifier for the purpose …' in clause 20(2)(b) of the Healthcare Identifiers Bill 2010 (Cth) be amended to read:*

    '(b) … healthcare identifier;
    for the purpose …'

13. *That the words '… use the healthcare identifier, or to disclose the healthcare identifier to a healthcare provider, for the purpose …' in clause 24(2) of the Healthcare Identifiers Bill 2010 (Cth) be amended to read:*

    '(b) … use the healthcare identifier; or
    (c) to disclose the healthcare identifier to a healthcare provider;
    for the purpose …'

Duty of confidentiality

PIAC is concerned about several aspects of the provision dealing with the service operator's duty of confidentiality.

Firstly, the offence provision in clause 15(1) applies only to a person (presumably an employee or officer of the service operator) who received information under Part 2, which deals with assigning healthcare identifiers, and Division 1 of Part 3, which deals with use and disclosure of identifying information for

assignment of healthcare identifiers, and then uses or disclosures that information for a purpose other than a purpose provided for under clause 15(2).

This does not capture use or disclosure of information by a person (who is an employee or officer of the service operator) where the information was disclosed to that person under clauses 16 in Part 3, Division 2 of the Bill. This needs to be remedied to ensure that the clause 15 covers all disclosures to the service operator.

It is also unclear whether or not the service operator can be 'a person' held liable under clause 15. Certainly, while Medicare is the service operator, the effect of clause 4(2) of the Bill seems to be that the service operator could not be held liable. This is a completely inappropriate limit on liability.

The provision also does not deal with a person who has obtained information through unauthorised accessing of the service operator's data system through, for example, computer hacking.

The legislative scheme should ensure that the service operator can and will be held either directly liable for unauthorised disclosure of information, or vicariously liable for unauthorised access to information by third parties or disclosure of information by it employees, officers or agents.

Such a provision providing for vicarious liability should, at minimum, be a provision that deems the service operator vicariously liable unless it can establish that it had sufficient security systems in place to avoid unauthorised access or disclosure and extensive training for employees and agents in respect of these obligations not to disclose information except as authorised under the legislation.

Further PIAC is concerned about the scope of the exemption in clause 15(2)(b) as there is no limit on laws that could authorise disclosure. PIAC notes that the term 'law' is defined in clause 5 to include not only Commonwealth Acts and legislative instruments, but also the Acts and legislative instruments (including delegated legislation) of all of the States and Territories.

Recommendations

14. *That the Healthcare Identifiers Bill 2010 (Cth) be amended to remove the crown indemnity in clause 4(2) so as to ensure that if the service operator is an entity of the 'crown' it can be held liable for breaches of the legislation.*
15. *That the Healthcare Identifiers Bill 2010 (Cth) be amended to ensure that the service operator can be held jointly and severally liable with other persons for breaches of the legislation where the breach occurred as a result of actions of an employee, officer or agent of the service operator or due to a failure of the information security systems of the service operator. This could take the form of a provision in the following terms:*
    - *(a) The service operator is to ensure that its officers, employees and agents are made aware of their obligations and the legislative limits in respect of the authorised collection, use and disclosure of information and healthcare identifiers under this Act.*
    - *(b) The service operator is to take reasonable steps to ensure that no officer, employee or agent of the service operator engages in conduct that is in breach of their obligations and*

legislative limits in respect of the authorised collection, use and disclosure of information and healthcare identifiers under this Act.

(c) The service operator is to take all reasonable steps to ensure that all information and healthcare identifiers are secured against access, use or disclosure that is not authorised under this Act.

(d) If the service operator does not comply with subsections (a) or (b) it is liable for any contravention of this Act committed by any of its officers, employees and agents.

(e) If the service operator does not comply with subsection (c) it is liable for any contravention of this Act resulting from unauthorised access to information or healthcare identifiers.

16. That the Healthcare Identifiers Bill 2010 (Cth) be amended either:

(a) to remove clause 15(2)(b); or

(b) to reword clause 15(2)(b) to read 'a purpose that is expressly authorised under a prescribed law'.

Disclosure of healthcare identifiers

There are provisions that provide for authorised disclosure of healthcare recipient healthcare identifiers:

- Clause 17(1) authorises the service operator to disclose a healthcare identifier to a healthcare provider.
- Clause 24(1) authorises a healthcare provider to disclose a healthcare identifier to 'an entity'.

PIAC considers that the term 'entity' in clause 24(1) is unduly broad and would permit disclosure to any person or organisation. Partnered with the purposes set out in clause 24(1)(a) and 24(1)(b), there is little limiting the potential recipients of healthcare identifiers.

This provision appears to permit, for example, a medical practice to disclose a healthcare recipient's healthcare identifier to a university (being an 'entity') for research purposes (under clause 24(1(a)(iv) and the university could in turn disclose the healthcare identifier to a second medical practice for medical research.

In addition to its recommendations 4 to 6 above, PIAC urges the Committee to consider limiting the scope of disclosure under clause 24.

In respect of use or disclosure of a healthcare identifier, PIAC notes that clause 24(1)(b) was not included in the Exposure Draft Bill and provides for use or disclosure that is reasonably believed to be 'necessary to lessen or prevent (i) a serious threat to an individual's life, health or safety; or (ii) a serious threat to public health or public safety'. PIAC notes that this additional permissive use or disclosure reflects a contentious element of proposed changes to the Privacy Act and urges the Committee to either remove this subclause from the Bill or limits its scope to 'serious and imminent' threats.

Recommendation

*17. That the Healthcare Identifiers Bill 2010 (Cth) be amended either to remove clause 24(1)(b) or change the wording of paragraphs (b)(i) and (ii) to read 'serious **and imminent** threat'.*

Liability for disclosure of healthcare identifiers

Clause 26 provides for offences in respect of use or disclosure of healthcare identifiers for purposes other than for the purposes authorised under the Act[15] or 'for a purpose that is authorised under another law'.[16] As noted above under 'Duty of confidentiality', the second exception is unduly broad and should be limited through amending it to read 'for a purpose that is **expressly** authorised by a **prescribed** law'.

Further, PIAC presumes that the exception to liability found in clause 26(2)(c) is designed to permit a healthcare recipient or a person responsible for a healthcare recipient to use or disclose their own healthcare identifier. This is not, however, entirely clear and could usefully be amended to provide certainty.

Recommendations

18. *That the Healthcare Identifiers Bill 2010 (Cth) be amended either:*
    - *(a) by the removal of clause 26(2)(b); or*
    - *(b) by amendment of clause 26(2)(b) to read '… for a purpose that is expressly authorised under a prescribed law'*
19. *That clause 26(2)(c) of the Healthcare Identifiers Bill 2010 (Cth) be amended to read:*

    the healthcare identifier is the healthcare identifier allocated to the person or to a person for whom the person is the person responsible (within the meaning of subclause 2.5 of National Privacy Principle 2) and the person uses or discloses the healthcare identifier only for the purpose of, or in connection with, the person's personal, family or household affairs …

Prosecution of offences

PIAC is concerned that offences under the legislation are unlikely to be prosecuted unless there is a specific prosecuting authority. A strong message needs to be sent that such breaches are extremely serious and will be acted on. PIAC holds this concern based on its experience in the area of anti-discrimination law where there are offences specified in various of the federal anti-discrimination statutes, the oldest of which came into effect in the 1970s. As far as PIAC is aware there has never been a prosecution of an offence under any of these statutes. It is PIAC's understanding that such prosecutions, as with prosecutions under the Bill in its current form, would have be to pursued by the Federal Director of Public Prosecutions.

While clause 29 provides that a contravention of the legislation 'in connection with the healthcare identifier of an individual is taken to be … for the purposes of the *Privacy Act 1988*, an interference with the privacy of an individual', this is not enough. Firstly, it only deals with contraventions in relation to healthcare identifiers and should also deal with contraventions in relation to identifying information. Second, without an accessible and targeted prosecuting body, the burden of dealing with offences under the will fall on the individual affected by the breach with their only option being to bring a complaint under the Privacy Act. In this circumstance, any penalty that the legislation imposes for an offence cannot be pursued through the individual complaint mechanism.

---

15 Healthcare Identifiers Bill 2010 (Cth) cl 26(1) and (2)(a)(i).

16 Healthcare Identifiers Bill 2010 (Cth) cl 26(1) and (2)(b).

Consideration should be given to strengthening and clarifying the process for prosecution of offences and to linking a successful prosecution with a positive finding of breach of the Privacy Act in favour of an affected individual, enabling a remedy to flow to the individual.

In addition, as with the proposed liability on the service operator for failure to ensure compliance with the Act and security of data, PIAC urges the Committee to include a provision in similar terms in respect of protection of healthcare identifiers.

Recommendations

20. *That the Senate Community Affairs Legislation Committee specify a prosecuting authority in respect of offences under the Act.*

21. *That clause 27 of the Healthcare Identifiers Bill 2010 (Cth) be amended to ensure that entities can be held jointly and severally liable with other persons for breaches of the legislation where the breach occurred as a result of actions of an employee, officer or agent of the entity or due to a failure of the information security systems of the entity. This could take the form of additional subclauses in clause 27 in the following terms:*

    (c) ensure that its officers, employees and agents are made aware of their obligations and the legislative limits in respect of the authorised collection, use and disclosure of healthcare identifiers under this Act;

    (d) take reasonable steps to ensure that no officer, employee or agent of the entity engages in conduct that is an offence or in breach of their obligations and legislative limits in respect of the authorised collection, use and disclosure of healthcare identifiers under this Act.

    If an entity does not comply with subsections (c) or (d) it is jointly and severally liable for any contravention of this Act committed by any of its officers, employees and agents in respect of healthcare identifiers it holds.

    If an entity does not comply with subsection (a) it is liable for any contravention of this Act resulting from unauthorised access to healthcare identifiers the entity holds.

Publication of annual reports

PIAC commends the Department of Health and Ageing (DoHA) for amending the Bill to include obligations on both the service operator and the Privacy Commissioner to prepare annual reports in respect of the operation of the legislation and for those reports to be tabled in Federal Parliament.

PIAC suggests that the Committee require that such reports include reporting on any unauthorised access, use or disclosure of either identifying information or healthcare identifiers.

Other matters

PIAC notes that the definition of 'entity' in clause 5 of the Bill does not include corporate entities. In the context of the range of uses of the term 'entity' in the Bill, the meaning should be extended to include bodies corporate. For example, the definition of 'healthcare provider' in clause 5 indicates that it 'means' individuals and entities that conduct an enterprise that provides healthcare. By excluding corporate entities

from the meaning of entity, healthcare provider cannot under clause 5 include private corporations that conduct an enterprise that provides healthcare.

Recommendation

22. That the definition of 'entity' in clause 5 of the Healthcare Identifiers Bill 2010 (Cth) be amended to include bodies corporate.

Conclusion

As PIAC observes above and in its submission in response to the Exposure Draft Bill, there are a number of matters set out in this Bill that should be deferred until amendments to the Privacy Act have been finalised and other aspects of the Healthcare Identifier Service have been further developed.

The Bill is premature and PIAC urges the Committee to consider recommending that it be deferred until these matters have been finalised.