office of the privacy commissioner
new south wales

Committee Secretary
Senate Standing Committees on Community Affairs
PO Box 6100
Parliament House
CANBERRA ACT 2600

Enquiries: Siobhan Jenner
Tel: (02) 8019 1603
Our ref: A11/0385

By email: community.affairs.sen@aph.gov.au

Dear Committee Members

Re: Submission on the Personally Controlled Electronic Health Record Bill & Explanatory Memorandum

Thank you for providing an extended period of time in which to make a submission on the Personally Controlled Electronic Health Record Bill (the PCEHR Bill). I am grateful for the opportunity to provide the following comments on the privacy impacts and other matters arising in the PCEHR Bill. These comments are provided in accordance with my powers under section 36(2)(g) of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act).

We have provided submissions on the various stages of what has now evolved into the PCEHR system and PCEHR Bill. At certain points in that evolution we have been concerned by the rapid nature of the consultation, particularly in relation to the Concept of Operations documents, the Legislation Issues paper and the Exposure Draft of the PCEHR Bill and now the PCEHR Bill. Given the significance of this national public/private infrastructure, which has the potential to affect every individual in Australia, I would have expected longer consultation periods for each iteration, in order to allow stakeholders to fully consider and respond to the legal and operational mechanisms put forward.

Context

The *Healthcare Identifiers Act 2010 (Cth)* mandates the allocation of a Healthcare Identifier to consumers and providers of health services by the Service Operator. To some extent this process has been carried out or continues to be carried out for all 'identifier recipient's' as per the provisions of the *Healthcare Identifiers Act 2010 (Cth)*.

Under the PCEHR Bill, consumers may apply for registration. Only consumers with a healthcare identifier are eligible for registration. Registration appears contingent on

consenting to the uploading to the PCHER System any record that includes health information, however that requirement is varied by the consumer nominating a particular record or type or classes of records to exempt from uploading to the system. As discussed below this process, and how it works in practice remains somewhat unclear from the information provided to this Office. In making this point I note that much of detail of the PCHER System (and any consent, privacy and completeness of records issues), will only be determined once a significant number of consumers and providers have 'subscribed' to the system and it's effectiveness in respect of the objects of the various related Acts, can be measured and assessed. It may be that the contextual observations above are incomplete, but for some of the reasons explained earlier (and above), on current advice and available resources, the full import of the System remains unclear.

Governance

As we have previously submitted, this Office does not support the proposed federated governance model for the PCEHR system. While the Bill makes the System Operator the primary governance entity (subject to advice and review by Jurisdictional Advisory Committee and the Independent Advisory Panel), the governance model is fragmented with respect to dealings with personal and health information flows, particularly those matters not proscribed by the Bill which regulate the flows of personal and health information. The Explanatory Memorandum to the Bill states that the System Operator will be subject to the *Privacy Act 1988* (Cth) (the Privacy Act) and that 'other participants of the PCEHR system will be either subject to the Privacy Act or a designated state or territory privacy law'[1]. This leaves open the possibility that the personal and health information in the PCEHR system could be dealt with inconsistently across Australia. Such inconsistencies would be likely to arise in the day-to-day decision-making about collection, use and disclosures not provided for in the Bill. For instance, certain matters included in the access provisions for the private sector in the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act) are not mirrored in National Privacy Principle (NPP) 6 of the *Privacy Act 1988* (Cth) or in Part 4 of the Bill[2]. In my view these differences cannot be easily glossed over as they could result in very different outcomes for the same conduct depending on the jurisdiction in which the matters arises.

It is also possible that inconsistencies will arise in the context of complaint handling by State, Territory and Commonwealth privacy regulators. Inconsistencies in outcomes for complaints could lead to the perception of unfairness in the context of health privacy complaints arising under the PCEHR system, notwithstanding the application of different standards arising from the same or similar facts. We again suggest that in order to avoid these inconsistencies there should be a separate PCEHR privacy legislation/framework applying equally to all PCEHR participants, private and public, small and large business, health care providers and system operators which would displace the existing privacy obligations only to the extent that they concern matters relating to the operation or administration of the PCEHR

[1] Personally Controlled Electronic Health Records Bill 2011, Explanatory Memorandum at page 35. I note that this is not reflected in the Bill itself.
[2] See section 25 of the HRIP Act.

system. In our view a PCEHR oversight body, other than the System Operator or the Office of the Australian Information Commissioner would be in a position to deal with these privacy-related matters and with other complaints arising from the operation of the PCEHR system. Having an independent but comprehensive mandate would mean that this oversight body would bring independence, consistency and fair dealings to bear on its decision-making.

The Opt-in model

The cornerstone for a shared electronic healthcare system is the capacity for individuals to opt-on to such a system. In this regard, I am pleased to note that the Bill's stated Object is to 'enable the establishment and operation of a *voluntary* national system for the provision of access to health information relating to consumers of healthcare…'. However, I am concerned that while participation may be said to be voluntary, it will not necessarily offer individuals control over their health information at the point of registration. For instance clause 41(3) in Part 3 Division 1 of the Bill provides that 'consumers' must agree to the uploading of their health information by 'a registered health care provider organisation' unless they request in writing that 'a particular record, all records or a specified class of records must not be uploaded'. This means that individuals will need to take active measures to have certain information withheld from the system. For this to be meaningful, the individual must be made aware of the items of information that would / will be uploaded. It would be preferable to allow individuals to actively understand what information is available to be uploaded and then allow them to nominate what, if any, information will be uploaded and be viewable, so that the individual more actively controls the uploading of health information into the PCEHR system not merely the subsequent uses of that information.

Rules v Law

In a number of places the PCEHR Bill refers to Rules to be made by the Minister in relation to certain matters. While Part 4 Division 2 of the PCEHR Bill sets conditions relating to access controls and clause 46(2) prohibits the refusal of treatment or discrimination on the basis of a consumer's access controls and clause 109 provides that the PCEHR Rules may 'specify access control mechanisms', none of these provisions provide a legal entitlement for individuals to set access controls or to adopt a pseudonym when registering as a PCEHR consumer. In our view, matters which go to the stated aim of providing personal control by the consumer should be prominent and protected under the substantive law, not in a disallowable instrument such as a Rule made by the Minister. To this end we suggest that the PCEHR Bill should clearly articulate the rights of individuals to set their access controls and to a choose pseudonym[3] at the point of registration.

Notification

[3] Noting that this is subject to the requirement that the individual has already obtained a pseudonymous Individual Healthcare Identifier.

While the PCEHR Bill imposes limitations on particular collections, secondary uses and disclosures and the security of health information in the system, it does not reflect all the protections offered by the privacy principles in the Privacy Act or the HRIP Act. For instance there are no requirements in the Bill requiring notification about matters relating to the collection of health information (as in National Privacy Principle (NPP) 1.3 and in HPP 4) or the means by which individuals may dispute the accuracy of the information, as may arise where information about a third party may inadvertently be included in the system. It is also important that individuals be notified (possibly in an abbreviated form) about the potential uses and disclosures of their health information, such as those contained in clauses 63 to 70 of the PCEHR Bill. In my view, the obligations relating to the notification of individuals should not be relegated to Rules or to a default requirement to comply with the NPPs. Embedding the notification requirements in the PCEHR Bill is more likely to make participants aware of the importance of involving individuals in the control of their health information. Some disclosure provisions appear contrary to general provisions relating to the rules and law relating to proceedings and litigation (Eg: Clause 70 (1) (e)). Other provisions utilise somewhat ambiguous or otherwise unnecessarily ill-defined terms (eg: 'serious improper conduct' as drafted in 70 (1) (d) etc).

Penalties

Clause 74 provides a civil penalty to be imposed on registered healthcare practitioner organisations if:

(a) an individual requests access to a consumer's PCEHR on behalf of or purportedly on behalf of the registered healthcare provider; and
(b) the individual does not give enough information to the System Operator to enable the System Operator to identify the individual who made the request without seeking further information from another person.

From this it appears that registered healthcare practitioner organisations will be held responsible for the actions of an individual who requests a consumer's PCEHR but fails to provide sufficient information to enable the System Operator to furnish the request. This purpose of this clause is unclear. Firstly it is unclear how the individual would be authorised to make the request on behalf of the registered healthcare practitioner organisations, and secondly it is unclear why the failure to do so should result in the imposition of a penalty, when the problem could be easily remedied by requiring the healthcare provider organisation to provide further information in order to furnish the request.

In conclusion, this Office has, and will continue to support measures to enable the establishment and operation of an electronic health records system across Australia. In our view the privacy enhancing benefits of a shared electronic healthcare will outweigh the potential privacy impacts of the PCEHR system as long as those impacts, both legal and operational are identified and resolved before

implementation. I hope the foregoing comments in this submission will assist you in setting the legal parameters to achieve that goal. I thank you again for the opportunity to provide a submission on the PCEHR Bill.

Yours sincerely

John McAteer
Deputy Privacy Commissioner
Information and Privacy Commission