office of the privacy commissioner
new south wales

PCEHR legislation Issues Feedback
Department of Health and Ageing
GPO Box 9848
CANBERRA ACT 2601

Enquiries: Siobhan Jenner
Tel: (02) 8019 1603
Our ref: A12/0574

By email: ehealth.legislation@health.gov.au

Submission on the Personally Controlled Electronic Health Record System (PCEHR): Proposals for Rules and Regulations

We welcome the opportunity to make a submission on the PCEHR Proposals for Rules and Regulations (the Proposals document). While this Office has consistently expressed the view that dealings with the personal and health information of consumers participating in the PCEHR should be subject to privacy regime administered by an independent governance body, whose role should include dealing with privacy complaints as well as operational matters, we acknowledge that the PCEHR Act will contain some privacy protections (such as limits on collection use and disclosure) and that certain other privacy protections are to be contained in rules or regulations such as those in the Proposals document. The policy reasons for deciding which parts of the health information life-cycle are governed by legislation, regulation or rule have not been made clear to date, and in our view matters such as comprehensive notification, the right to request amendment of personal or health information and provision for pseudonymity and/or anonymity should be provided for by substantive law. Our comments below touch on some of those information life-cycle issues, which in our view should be provided for by regulation rather than rule as the former provides greater rigour and scrutiny and is less likely to be subject to change or deletion than a rule. In our view the Ministerial Council would provide greater rigour than Jurisdictional Advisory Committee would thus give the PCEHR privacy protections greater force.

Governance

3.1: The Proposals document states that one of the System Operator's responsibilities will be the management of complaints. Section 73 of the Bill provides that a contravention of the PCEHR Bill gives rise to 'an interference with privacy' for the purposes of the *Privacy Act 1988* (Cth) (Privacy Act). At the sixth bullet point at section 3.1 the Proposals document states:

> …the Office of the Australian Information Commissioner (OAIC) and where relevant, state and territory privacy and health information regulators will provide regulatory oversight, advice and carry out investigations in relation to PCEHR privacy issues…

Notwithstanding the work currently being undertaken by the Office of the Australian Information Commissioner (OAIC) to clarify the PCEHR complaint handling pathway,

it is unclear how this Office as the regulator responsible for administering privacy and health privacy law in New South Wales, could have legal standing to deal with an alleged interference with privacy under the Privacy Act by virtue of an alleged breach of the PCEHR Act. If the System Operator is responsible for managing complaints it will be necessary to clarify this and to also clarify whether it will be necessary for the System Operator is to attempt to resolve privacy complaints at first instance, given the operation of section 40(1A) of the Privacy Act[1].

Privacy & Access control mechanisms

3.3 & 5.2: The discussion in the Proposals document relating to privacy refers to the current requirements in the PCEHR Bill governing the collection, use and disclosure of consumers' information. One of the other key features of privacy law throughout Australia is the requirement to notify individuals at the point of collection how their information will be dealt with and protected. This gives individuals the opportunity to opt out of such dealings if they are not satisfied that their privacy will be safeguarded. If there is to be no such requirement in the PCEHR Act, it is critical that the PCEHR regulations (rather than the rules) governing the PCEHR system should require that individuals be provided with sufficient information about the PCEHR system at the point of enrolment in order to truly opt into the PCEHR system. In our view these matters would form part of the access control measures.

3.4 & 4: We support the provisions in the PCEHR Bill which enable consumers to view their PCEHR audit trail, however we suggest that there should be explicit reference to the fact that unauthorised access or alteration revealed in audit trails will constitute an interference with privacy[2], which in turn will give rise to the ability to make a privacy complaint.

Rules: Access control

5.2 (c) & (d): It is not clear from the Proposals document whether in circumstances where an individual 'hides' the existence of their PCEHR how a healthcare provider organisation will know to search the system in order to override the hiding mechanism in serious threat situations.

The period of 5 days for allowing access in case of serious threats is far too long in our view, let alone the apparently unlimited 'repeat as necessary' extensions. A serious threat is generally an imminent threat; the less imminent, the less serious. If the threat is of a medical nature the healthcare provider organisation should ensure that the consumer is either treated immediately at the scene or is transported to an Accident and Emergency centre for treatment. If the threat is of a security nature the healthcare provider organisation should contact the Police. In any case if a serious

[1] This provision requires that the Privacy Commissioner decline to deal with a complaint if the matter has not first been raised with the respondent organisation (subject to an appropriateness test).
[2] As provided for in clause 73 of the PCEHR Bill.

threat goes beyond these circumstances this it is unlikely to be imminent and therefore unlikely to be serious or to be a threat in the health context.

5.2(e): The discussion about access control mechanisms in this section describes the technical requirements which will apparently reflect the consumers wishes with regard to which practitioners can see what information. However, it appears that the emphasis is less on what consumers have chosen and more on the rights of healthcare provider organisations and other participants:

> …all healthcare provider organisations that are part of, or subordinate to, the first provider will have the same access rights as the first provider…
>
> …the System Operator may direct the seed organisation to amend the access flags applicable to its network hierarchy…
>
> …the System Operator will be able to establish and maintain other access control mechanisms, provided that such mechanisms are consistent with the PCEHR Bill and the requirements specified in the rules…

If it is not practicable to allow consumers to set all access controls then this should be made patent at the point of enrolment.

Identity verification

5.3: The Bill requires that the System Operator must have regard to matters specified in the PCEHR rules relating to the identification of a consumer when registering the consumer. We support the suggestion in the Proposal document that as a base line requirement consumers should have a verified individual healthcare identifier (IHI). We suggest that this should be supplemented with primary secondary documents sufficient to establish a 100 point Austrac check.

Participation requirements

5.5.1: The Proposals document suggests that healthcare provider organisations must develop, maintain, enforce and communication policies and procedures about their access to the PCEHR system. In our view some of the matters listed in this section should be mandated by regulation rather than by localised policy and procedure documents. This is especially true in relation to the following listed matters which go to the protection of consumer information and to access controls:

- the manner of authorising persons within the organisation with access to the system
- the process for identifying a person authorised to access the system and providing identification information to the System Operator
- protection and security of IT equipment and related resources from unauthorised access

- the use of physical and system access controls, such as user identification, passwords and digital certificates…

We also suggest that the privacy protections in the PCEHR Bill and those to be provided for by rules and regulations should be contained in a privacy policy, disseminated to staff and made available to consumers each time they access their PCEHR. The privacy policy should outline the penalty provisions in the Bill and describe the pathway for consumer privacy complaints.

Thank you again for the opportunity to make these submissions on the PCEHR Proposals document and I trust my comments will be of assistance to you in developing the PCEHR rules and regulations.

Yours sincerely

John McAteer
Deputy Privacy Commissioner
Information and Privacy Commission