PRIVACY IMPACT ASSESSMENT OF THE PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORD SYSTEM RESPONSE TO RECOMMENDATIONS BY THE DEPARTMENT OF HEALTH AND AGEING

The Department has committed to a thorough and robust examination of the Personally Controlled Electronic Health Record (PCEHR) system, throughout its development. As part of this commitment, the Department engaged Minter Ellison Lawyers, in conjunction with Salinger Privacy, to conduct a privacy impact assessment (PIA) of the current design of the system and legislation.

The PIA identifies a wide range of privacy positives and risks for the PCEHR system, and puts forward 112 recommendations for managing the identified risks. The Department has accepted the majority of recommendations in full, with many others accepted in principle or in part. A breakdown of the Department's response into categories is provided in the table below.

Response type	Accept	Accept in principle	Accept in part	Supported	Under consideration	Not accepted
Number of responses	75	20	6	2	1	8

The Department has approached the recommendations in the following way:

1. **Accepted** – the Department accepts the recommendation in full;

2. **Accepted in principle** – the Department accepts the recommendation's intent and general framework. This response most commonly occurs when a recommendation involves content being included in principle legislation, when the Department considers that subordinate legislation or contractual arrangements are a more appropriate vehicle for the enforceable obligations;

3. **Accepted in part** – the Department substantially accepts only some of the components of the recommendation;

4. **Not accepted** – the Department does not accept the recommendation, however in the six cases where implementation would be feasible the Department would seek the views of the Senate Community Affairs Committee in conducting its inquiry into the PCEHR Bills;

5. **Under consideration** – the Department is investigating further before making a response. This response reflects situations, for example, where the recommendation needs to be tested for technical feasibility; and

6. **Supported** – the Department considers the recommendation has merit, but it relates to the actions of other organisations such as the Australian Information Commissioner and Healthcare Identifiers Service Operator.

The Department provides a response to each recommendation individually below.

PHASE 1 RECOMMENDATIONS

No.	Recommendation	Response	Discussion
4.1	That the PCEHR Bill include the requirement for a consumer (or their Authorised Representative)'s express consent to register for a PCEHR	Accepted	The opt-in nature of the PCEHR system is implicit in the legislation to support it, ie, the System Operator may only register a consumer for a PCEHR where he or she has applied (s39 and s41). A note has been included in the legislation (s41) to draw attention to this consequence of the legislation.
4.2	That the PCEHR Bill not allow regulations or other subordinate legislation to create an exemption from the express consent requirement.	Accepted	The legislation does not provide any mechanism for making exceptions to the opt-in nature of the PCEHR system (s41).
4.3	That any plans for transition of data from existing shared EHR systems incorporate a 'fresh' express consent process.	Accepted	The Department will be looking at ways to make it as easy as possible for consumers to transition from existing electronic health record systems to the PCEHR system, if this is what they want to do. This is clearly dependent, however, on the consumer having made a decision to join the PCEHR system.
4.4	That the PCEHR Bill prohibit: (1) inducing a consumer to register for a PCEHR (other than by reference to the benefits of the PCEHR itself); (2) inducing a consumer to provide a copy of their PCEHR to a third party; (3) consumers being placed at a disadvantage (financially or in relation to access to healthcare) if they do not have a PCEHR; and (4) consumers being placed at a disadvantage (financially or in relation to access to healthcare) for declining to provide permission for a healthcare provider to access their PCEHR.	Accepted in principle	The Department has designed a system which has the voluntary participation by consumers at its core. The approach in the legislation is to reinforce this design feature, including a 'no discrimination' rule which prohibits a healthcare provider from discriminating against a consumer because he or she does not have a PCEHR, or does not choose to provide the healthcare provider with access to it (s46). Other forms of discrimination are not expressly dealt with in the PCEHR legislation, because they are already covered by other legislation. For example, the ability to

No.	Recommendation	Response	Discussion
			discriminate between consumers who are applying for health insurance cover is already very limited and subject to parliamentary scrutiny. Similarly, the use and disclosure of healthcare identifiers for insurance underwriting and employment purposes is prohibited (s24 of the *Healthcare Identifiers Act 2010*). As a result, the Department does not propose to duplicate existing protections, but will instead highlight them in consumer communications.
4.5	That advice be provided to Conformant Portal Providers, to ensure that their marketing, privacy notices and terms and conditions clearly reflect the distinction between the PCEHR System and any services offered by the portal provider.	Accepted	Conformant Portal Providers will need to meet proper technical and procedural standards in order to be eligible to connect to the PCEHR system. These issues raised by the PIA will be taken into account in the development of the standards.
4.6	That there be a further review of the detailed plans for online registration, to ensure the online channel offers a similar level of privacy protection as the assisted registration channels, particularly in terms of collection necessity and data security.	Accepted	The development of the PCEHR system has been an iterative process, with the evolving design being tested regularly along the way. This testing has been both through public consultation – such as the release of the draft Concept of Operations and Legislative Issues paper – and through internal review. This has continued with the release of exposure draft legislation for public consultation, and there is to be ongoing internal review of the detailed plans for all aspects of the system.
4.7	That the PCEHR Bill clearly describe the type of information to be used and disclosed to verify consumer identity, by whom it will be used or disclosed, and for what purposes.	Accepted in part	The Department sees this recommendation as being directed towards two privacy objectives. These are to: • Provide consumers and bodies handling this demographic information with clarity around how this information may be used and disclosed; and • Provide a framework for proper use and disclosure.

No.	Recommendation	Response	Discussion
			The Department agrees that these are important objectives which should be met, but not that specifying these in the legislation is the optimal method for achieving these. The Department is concerned that a prescriptive approach to what information may be used to assert identity to the PCEHR system may unnecessarily disadvantage some consumers. Using a policy based framework instead, there is the flexibility to provide access to the system to consumers who may have difficulty asserting their identity using the generally recognised kinds of documents. Using a policy based framework, the bodies handling the information would still be restricted under law to collecting information necessary for the purpose of registration. Collection of irrelevant information would be a breach of the *Privacy Act 1988* (Cth) (see Information Privacy Principle 1.1, National Privacy Principle 1.1). Accordingly, the Department does not accept the part of this recommendation relating to the types of information that may be collected. In relation to placing a framework around how information collected during the registration process may be used and disclosed, the Department considers that this recommendation has merit. To make the PCEHR system accessible to the community, multiple channels for consumer registration are being developed. It is a sensible and equitable measure to have the information collected treated consistently, irrespective of the channel chosen by the consumer (s58). The Department considers that this framework is better supported by subordinate legislation or terms and conditions of participation, because these provide greater

No.	Recommendation	Response	Discussion
			speed and flexibility in dealing with any emerging issues in the registration process.
4.8	That there be a further review of the detailed plans for face to face registration of a minor, to ensure the face to face channel offers a similar level of privacy protection as the online channel, particularly in terms of data security and association to the correct guardian.	Accepted	The Department will continue to review all aspects of the PCEHR system about how they will operate in practice.
4.9	That there be a further review of the purpose of asking 'challenge and response' questions, noting that verification can alternatively occur by entering an IVC number, irrespective of whether the questions are answered correctly.	Accepted	The Department has reviewed this part of the registration process. While there is a place for the IVC number to be used, it is also essential that challenge and response questions are able to be used both for registration and access.
4.10	That Authorised Registration Agents (ARAs) for the PCEHR be encouraged to utilise the national Document Verification Service, instead of recording details of the EOI documents presented.	Under consideration	The Department is investigating whether and how the Document Verification Service might be used to support the registration processes of the PCEHR system.
4.11	That the PCEHR Bill provide that ARAs for the PCEHR may not keep copies of EOI documents, and that any such copies must be securely destroyed as soon as the registration process is complete.	Accepted in principle	The Department accepts that registration processes have the potential to create a concentration of identification documents, which represents a privacy risk for consumers. The Department agrees that collection and retention of identification documents of ARAs needs a clear framework. Detailed arrangements for management of information by ARAs will not be specified in the principal legislation. This kind of detail is more appropriate for subordinate legislation, or contractual arrangements between the system operator and the ARAs.
4.12	That the PCEHR Bill clarify whether ARAs for the PCEHR may or must keep a record of the EOI document number.	Accepted in principle	Please see comments against recommendation 4.11

No.	Recommendation	Response	Discussion
4.13	That the PCEHR Bill require consumers seeking to register via mail to post certified copies of the EOI documents (not just a statement from a JP about sighting the documents).	Accepted in part	The Department confirms that postal registration will require the provision of certified copies of documents, rather than just a statement from a justice of the peace or other person that they have sighted identity documents. This will not, however, be required in the principal legislation. The Department considers that fixing details of administrative processes such as registration in legislation has the potential to be counter-productive, because it: ▪ reduces the speed at which the system operator can act to address any emerging security or other problems with a registration channel; and ▪ makes it more difficult for the system operator to refine processes over time so that they are more efficient and effective. Instead, the Department considers that a rigorous framework around the development of processes and operational policy by the system operator is the better approach (see recommendation 8.19).
4.14	That the arrangements with ARAs ensure that there are physical privacy protections for consumers using their shop fronts, such as timed logouts and privacy screens on public-facing computers.	Accepted	The Department considers that these are all effective and practicable means of providing privacy protection for consumers in a shopfront environment.
4.15	That the arrangements with ARAs ensure that there are administrative and technical privacy protections, such as appropriate staff screening, staff training in privacy obligations, and audit logging of staff registration transactions.	Accepted	The Department considers that these are key aspects of the delivery of registration services, and will build these into the assessment of ARA candidates and the monitoring of the performance of engaged ARAs.
4.16	That the PCEHR Bill provide that in order to register an adult consumer, an Authorised Representative must provide:	Accepted in	The Department agrees that there needs to be a robust

No.	Recommendation	Response	Discussion
	• certified copies of 100 points worth of evidence of their own identity; • certified copy of documentary evidence of legal authority to act on behalf of the consumer eg • certified copy of guardianship order; • the Medicare card of the consumer; and • where the evidence of their position as a representative of the adult consumer is unclear as to the consumer's current state of capacity, further evidence that the consumer currently lacks the capacity to make a decision about registration, or manage their PCEHR, themselves.	principle	framework around the participation by authorised representatives, which ensures that: ▪ the authorised representative does have a right to act on behalf of the consumer; and ▪ the authorised representative is associated with the right consumer. The Department does not consider, however, that the operational processes for achieving this should be fixed in the principal legislation, thereby reducing the ability of the system operator to be responsive to emerging threats, or consumer needs. The Department will take account of the model recommended when developing the more detailed specifications for assessing registration applications involving authorised representatives.
4.17	That communications to consumers explain the registration rules in relation to authorised representatives, including those appointed under enduring guardianship arrangements.	Accepted	Clear and accessible material about the participation of authorised representatives in the PCEHR system will be developed. The Department has engaged a National Change and Adoption Partner to assist with the development of communications material for consumers.
4.18	That the PCEHR Bill authorise the disclosure of each 'stream' of Medicare held data (MBS, PBS, organ donor status and/or childhood immunisation records) to a consumer's PCEHR, upon confirmation that the consumer has provided a positive consent to that 'stream'.	Accepted	The PCEHR legislation allows for the inclusion of Medicare data in a consumer's PCEHR, with his or her consent (s38). The data a consumer may consent to is: Medicare Benefits Scheme (MBS), Pharmaceutical Benefits Scheme (PBS), Australian Childhood Immunisation Register (ACIR) and Australian Organ Donor Register (AODR).
4.19	That the final design allow a consumer who consents to the MBS and/or PBS data stream to choose whether they wish the	Accepted	The Department agrees that the default position should be

No.	Recommendation	Response	Discussion
	data stream to include data already collected up to two years prior to the date of their consent, with the default position being 'no back dated data'.		that no historical data be included in a consumer's PCEHR.
4.20	That the PCEHR Bill clarify which data 'streams' can be populated with data that pre-dates the commencement of the consent decision.	Not accepted but seek Senate Committee's views	As noted in relation to recommendation 4.18, the PCEHR legislation will allow for the inclusion of MBS, PBS, ACIR and AODR data in a PCEHR. This authorisation will allow for some historical data, as well as prospective data, to be included. This data will not be included in a consumer's PCEHR as a matter of course. Rather, the consumer will choose what, if any, data of these kinds is included. The Department considers that this approach gives consumers greater control over the content of their own PCEHRs.
4.21	That consumer communications advise consumers who are concerned about the privacy of specific illnesses or episodes of care (such as a pregnancy termination), that unless they are very health literate and prepared to 'remove from view' specific data items, their best option may be to not consent to the disclosure of the MBS / PBS data streams into their PCEHR.	Accepted in principle	The Department is working with the National Change and Adoption Partner to develop a comprehensive suite of materials to assist consumers to make informed choices about how they participate in the PCEHR system. The Department will incorporate information about the effect of including MBS/PBS data into consumer materials.
4.22	That the default position for consumers be that the existence of their PCEHR will be 'flagged' within local clinical systems unless the consumer chooses otherwise.	Accepted	The Department considers that this is a sensible approach. By having the existence of the PCEHR 'flagged' in this way, healthcare providers do not have to ask each patient whether they have a PCEHR. If there is no 'flag', the healthcare provider proceeds with the consultation as normal. If there is a 'flag', then the healthcare provider may draw on it in accordance with the access controls set by the consumer.

No.	Recommendation	Response	Discussion
4.23	That there be a name change to the 'not findable' access control, to instead be called 'not flagged'. 4.53 option.	Accepted	If a consumer chooses the 'not findable' setting, then the fact that he or she has a PCEHR is not automatically flagged in a healthcare provider's local clinical system. This setting allows a consumer to exercise choice about which healthcare providers have access to his or her PCEHR, without having to remember a code or have a difficult conversation with a healthcare provider about why he or she does not want to give access to the PCEHR. While the existence of the PCEHR is not 'flagged', it does remain 'findable' – if the consumer decides to tell a healthcare provider that there is a PCEHR, the healthcare provider can then find it. As a result, the Department agrees that it is more accurate to describe this setting as 'not flagged' rather than 'not findable'.
4.24	That consumer communications carefully explain the practical limits of the 'Revoke' access control	Accepted	The Department agrees that consumer communications need to clearly explain privacy control settings to consumers, including their limitations.
4.25	That the PCEHR Bill prohibit healthcare organisations from recording a consumer's PACC or PACC-X for future use (i.e. in the event that the organisation is moved to 'Revoked' status).	Accepted in principle	The Department accepts unconditionally that healthcare providers should not record a consumer's PACC or PACC-X for future use. The Department does not consider, however, that the operational processes for achieving this should be fixed in the principal legislation but is investigating whether this is most appropriately addressed in subordinate legislation, or in terms and conditions of participating in the PCEHR system.
4.26	That one option for the range of optional consumer notifications (SMS messages or emails) should be to receive a notification if an organisation on their 'Revoke' list changes their HPI-O in some way.	Not accepted	The Department is pleased that the Privacy Impact Assessment has recognised the privacy positives which the Healthcare Identifiers (HI) Service can offer to electronic transmission of health records. The HI Service is a foundation element of e-health, which has been jointly

No.	Recommendation	Response	Discussion
			designed and funded by the Commonwealth, States and Territories to provide a robust foundation for health communications. The Department does not, however, consider that this recommendation would achieve its intended objective, which is to provide consumers with a greater ability to exclude particular individuals from accessing their records, through providing information about the structure of healthcare organisations. The HPI-O is a number issued by the HI Service operator to healthcare provider organisations. The HI Service operator requires a healthcare organisation to undergo an evidence of identity (EOI) process at the time the HPI-O is assigned, but there is no ongoing monitoring of the organisation's structure. This means that changes to organisation structure – such as the sale of existing or purchase of new businesses – would not be visible to the HI Service operator, or have an effect on the HPI-O. This means that the kinds of information which this recommendation seeks to capture would not be available to consumers through notifications about HPI-Os.
4.27	That the Department develop some incentive for organisations to set their HPI-Os (for the purposes of the Access List) at a level which reflects the management of records within the organisation itself.	Not accepted but seek Senate Committee's views	The Department considers that the healthcare provider organisations are best placed to determine how best to use HPI-Os to support their business operations. While the PCEHR system is an important e-health initiative which will make extensive use of healthcare identifiers to support security and data quality, healthcare identifiers also support other electronic transmission of health information. A healthcare organisation might, for example, also be involved in e-prescribing or telehealth.

No.	Recommendation	Response	Discussion
			This means that some organisations may find that using a more granular HPI-O structure (where, for example, a large hospital chooses to have HPI-Os for departments within the organisation) helps it to direct electronic records more effectively, while others may find that a single HPI-O works better with the organisation's business and processes. Both of these approaches are legitimate ways to manage data security and quality.
4.28	That consumer communications about the various privacy control settings and the limits to those settings be available to consumers before they decide to register for a PCEHR.	Accepted	The Department agrees that consumer communications need to clearly explain privacy control settings to consumers, including their limitations.
4.29	That consumers have available to them a 'preview' function which allows the consumer to see how their record will appear to other types of users depending on the access controls they set.	Accepted	The Department considers that this is a useful mechanism to assist consumers to make informed decisions about privacy settings.
4.30	That the design of the system include some prompt every few years (such as a screen prompt on next log in) to consumers with Nominated Representatives to review their choices and check the accuracy of their information.	Accepted	The Department considers that this would be a technically simple and effective method of both encouraging consumers to be engaged with their health records, and supporting the efficiency and effectiveness of the PCEHR system.
5.1	That the design of the PCEHR System allow the consumer's 'home address' field to be left blank, or accept postal box addresses.	Accepted	This recommendation reflects the current design of the PCEHR system, and the Department has no plans to change this. The Department notes, however, that it is possible that address information is included in clinical documents uploaded to a consumer's PCEHR. That is, while it may not be visible in the general or summary pages of the PCEHR, it may be visible in clinical documents which

No.	Recommendation	Response	Discussion
			have been attached to the PCEHR (such as discharge summaries or pathology reports).
5.2	That consumer communications advise consumers of their choices regarding the address entered in their PCEHR, but also warn them that their home address might be contained in clinical records indexed through the PCEHR.	Accepted	The Department agrees that consumer communications need to clearly explain privacy control settings to consumers, including their limitations.
5.3	That the design of the PCEHR System remind a consumer, at the point of data entry about their emergency contacts, that all other users including Authorised Representatives and nominated Representatives will see that data; that the PCEHR System provide a notice to consumers, recommending that consumers take reasonable and practical steps to obtain consent from those other people, where appropriate.	Accepted	The Department agrees that this is a sensible approach.
5.4	That a privacy notice be visible when a consumer seeks to enter data in their private 'Notes' area, explaining the circumstances (if any) in which third parties could gain access to that information.	Accepted	The Department agrees that consumer communications need to clearly explain privacy control settings to consumers, including their limitations.
5.5	That the design of the PCEHR System include a mechanism by which a consumer can exercise their privacy right of correction, by associating a statement with an indexed clinical document, such as through the Consumer Entered Health Summary.	Accepted	The design of the PCEHR system includes a mechanism to support correction of clinical documents included in a consumer's PCEHR, and also makes provision for the association of a statement with the clinical document. Instead, the current mechanism allows a consumer to remove a disputed record from his or her PCEHR. In order to remove a document, the consumer must indicate the reason for removing the record from three options: 1. The document is not about me; 2. The document content is incorrect; or 3. No reason given. If the consumer chooses option 1 or 2, the PCEHR

No.	Recommendation	Response	Discussion
			operator initiates investigative action as part of the removal. Where the consumer considers that the document is not correct, the PCEHR operator refers the document back to the healthcare provider who authored it for review. The document may then be reposted to the PCEHR system, when the consumer and healthcare provider are satisfied with its (possibly revised) content. The System Operator automatically associates a statement with the initially posted record – that the consumer disputes it content – and takes it out of circulation. Only a version of that document which has been reposted with the consent of the consumer will subsequently be made available to healthcare providers. The Department considers that this mechanism strikes a good balance between providing consumers with rights to exercise control over the content of their PCEHRs, and ensuring that the clinical content of the PCEHRs does not become diluted or confusing. The Department intends that communications provide adequate information about this facility.
5.6	That the design provide for appropriate anti-hacking measures such as a maximum number of attempts before the PCEHR System 'locks out' the consumer and that mechanisms are in place for consumers to then reset their password or be re-directed to an assisted channel (eg face to face or Telephone).	Accepted	The Department will ensure that high quality anti-hacking mechanisms and processes are included in the PCEHR system.
5.7	That consumers are given advice on the suitability of questions and answers, eg the answer should only be known by the consumer and the answer remains true over time.	Accepted	The Department considers that this is a useful way to support the security of consumers' PCEHRs, and will incorporate this recommendation in the development of communications material to consumers.

No.	Recommendation	Response	Discussion
5.8	That special authentication mechanisms are put in place for consumers with a Nominated Representative (to allow Call Centre employees to distinguish between the consumer and a Nominated Representative). To mitigate this, the importance of 'secret questions and answers' set at registration by the consumer must be clearly communicated to consumers ie do not record the answers in your PCEHR.	Accepted	The Department agrees that consumers and their nominated representatives need to be identifiable and distinguishable from each other in their communications with the PCEHR operator. The Department will examine how this can be achieved in a secure and effective way.
5.9	That the PCEHR Bill prohibit Conformant Portal Providers from recording a consumer's IHI.	Not Accepted, but seek Senate Committee's views	The Department considers that there are legitimate reasons for a portal provider to collect a consumer's individual healthcare identifier. For example, a portal may provide functionality which assists consumers with print disability, such as with a read aloud service. To do this may require the storage of information from the consumer's PCEHR itself, at least on a temporary basis. The Department agrees that proper rules should govern the conduct of a portal provider, to ensure that a consumer's identifier is protected from inappropriate use and disclosure. Just as for conformant repositories, any collection, use or disclosure of identifiers by a portal is limited to purposes which are related to the delivery of the PCEHR system (s22C Consequential Amendments Act).
5.10	That the design of the PCEHR System include a 'PCEHR-specific' portal, such that consumers need not expose their personal information to any other organisation in order to gain access to their PCEHR online	Accepted	The PCEHR operator will offer portal facilities for consumers.
5.11	That regulations under the PCEHR Bill set controls over the PCEHR System Operator's Call Centre including requirements for staff security screening the monitoring of calls and how much of a consumer's data can be 'viewed' in what circumstances.	Accepted	The Department agrees that a clear and robust framework is required for the operation of the PCEHR system call centre. The Department considers that this would be achieved in a flexible and responsive way through the use of regulations or rules. This is provided for in the legislation (s109(2) and (3)).

No.	Recommendation	Response	Discussion
5.12	That the design of the 'Authorised Representative' component of the PCEHR System be reconsidered, with a view to limiting the access of Authorised Representatives of adult consumers (and Authorised Representatives of children in some circumstances) to only viewing the Shared Health Summary and Consumer Entered Health Summary, rather than all clinical records.	Not accepted but seek Senate Committee's views	It is fundamental to the role of the authorised representative that he or she can manage the PCEHR in the same way as the consumer. In the absence of the authorised representative being able to do this, the consumer without capacity would not have a voice in dealings with the PCEHR system. The PCEHR system will make provision for a person to make decisions in relation to another consumer's PCEHR, when the consumer does not have the capacity to make decisions for him or herself. It will do this by recognising the kinds of arrangements courts and tribunals, and individuals themselves, put in place to authorise a person to 'stand in the shoes' of the consumer without capacity. This includes health-related powers of attorney and guardianship orders.
5.13	That the PCEHR Bill establish the eligibility rules for Authorised Representatives of both child and adult consumers, as well as providing the PCEHR System Operator with the ability to limit, suspend or revoke access rights of Authorised Representatives in accordance with an established protocol.	Accepted	The PCEHR legislation includes provisions which set out when one person may make decisions on behalf of another in relation to the PCEHR system (s6 and s7).
5.14	That the PCEHR System Operator develop a protocol for dealing with complaints by or about 'competing' Authorised Representatives, including the circumstances in which the PCEHR System Operator may limit, suspend or revoke access rights of Authorised Representatives, such as on presentation of evidence such as an apprehended violence order.	Accepted	The Department agrees that a protocol for dealing with conflict between authorised representatives is required, and will develop this.
5.15	That the design of the 'authorised representative' component of the PCEHR System include technological design and procedural protocols to ensure regular reviews (such as every three years) of the continued validity of instruments asserting	Accepted in principle	The Department agrees that the design of the system needs to support proper monitoring of the right of authorised representatives to continue to represent other consumers. The Department is still considering what is the appropriate

No.	Recommendation	Response	Discussion
	the eligibility of Authorised Representatives of adult consumers with intermittent or fluctuating capacity.		period for review of representation rights, and how to best monitor these in a risk managed and responsible way.
5.16	That the design of the 'authorised representative' component of the PCEHR System be reconsidered to allow some mechanism for adult consumers who have one or more authorised representatives to exercise their privacy rights (such as setting access controls or removing clinical records) while in a state of capacity. This mechanism would need to be time critical for example when in the presence of a healthcare provider who can make a judgment about their capacity at that immediate time.	Accepted	The Department agrees with having a mechanism or mechanisms in place to provide better support for those who have fluctuating capacity to make their own decisions when they are able, and be included in decision-making about them where possible when they do not have capacity. To provide support the legislation provides for a consumer who wishes, to allow a nominated representative to have the same level of control as an authorised representative – that is, be able to act on behalf of the consumer in relation to the consumer's PCEHR, including setting access controls to the consumer's PCEHR and granting consent to a healthcare provider organisation. (s7) This flexibility in setting access controls will take into account the many circumstances in which a person may not be able to, or may not wish to, manage their own PCEHR but does not have a formal legally recognised authorised representative to act on their behalf.
5.17	That the PCEHR Bill define 'employee' to explicitly include tertiary healthcare students on placement.	Not accepted but seek Senate Committee views	The definition of 'employee' as currently proposed covers tertiary healthcare students on placement without the need to expressly list them or include a new definition for a tertiary healthcare student. There is no need to add further text and therefore complexity to the legislation. The Department will include text about the participation of tertiary healthcare students in the explanatory memorandum, however, to explain how they fall within the definition of 'employee'. Whether tertiary healthcare students are in practice provided with access to the PCEHR system will reflect the

No.	Recommendation	Response	Discussion
			internal protocols of the healthcare provider organisation, and whether they have a legitimate reason to access the system as part of their placement duties.
5.18	That the PCEHR Bill define or include guidance as to what constitutes a 'legitimate need' for other individuals who do not have a HPI-I within a healthcare provider organisation to access the PCEHR System.	Accepted in principle	The Department agrees that there should be clear and practical guidance to healthcare provider organisations about when it is appropriate to allow 'an employee' to access the PCEHR system, as well as other key aspects of how they should manage their responsibilities to the PCEHR system. The Department is not convinced, however, that the principal legislation is the best place to achieve this. The Department considers that subordinate legislation or participation terms and conditions are better vehicles, because they provide better scope to be responsive to any emerging threats to the system.
5.19	That the PCEHR Bill set one of the conformance requirements on an HPI-O as an obligation to verify, with 100 points of EOI, the identity of each proposed user (and confirm their proper association to an HPI-I, where applicable).	Accepted in part	The Department agrees that conformance requirements for healthcare providers participating in the PCEHR system need to address procedural, as well as technical, security measures they need to take. The Department will test this option for managing identity of employees as part of developing conformance requirements. The Department considers that principal legislation is not the place for conformance requirements, either technical or procedural. Subordinate legislation provides much greater capacity for the PCEHR operator to take quick and decisive action to head off any emerging threat to the system.
5.20	That the PCEHR Bill set one of the conformance requirements on an HPI-O as an obligation to provide training to their employees on the appropriate access to and use of PCEHRs	Accepted in principle	The Department agrees that proper training for employees will need to be part of conformance requirements for healthcare provider organisations.

No.	Recommendation	Response	Discussion
	including the 'PCEHR privacy rules' and any other privacy obligations applying to that organisation.		The Department considers, however, that principal legislation is not the place for conformance requirements, either technical or procedural. Subordinate legislation provides much greater capacity for the PCEHR operator to take quick and decisive action to head off any emerging threat to the system.
5.21	That the PCEHR Bill ensure that the 'PCEHR privacy rules' must be confirmed as understood and accepted by individual users as a condition of their first access to the PCEHR System.	Accepted in principle	The Department considers that this is properly part of the conformance requirements of healthcare provider organisations. The Department considers, however, that principal legislation is not the place for conformance requirements, either technical or procedural. Subordinate legislation provides much greater capacity for the PCEHR operator to take quick and decisive action to head off any emerging threat to the system.
5.22	That consumer communications draw attention to the fact that under the 'Basic' access controls, any authorised user of the system can find their PCEHR so long as the user knows at least the consumer's full name, gender, date of birth, and either their address or their Medicare / DVA number.	Accepted	The Department agrees that consumer communications need to clearly explain privacy control settings to consumers, including their limitations.
5.23	That when designing the conformance tests for clinical software seeking to interface with the PCEHR system, the Department and NEHTA give consideration to how a PCEHR can be 'found' in an automated way, with a view to ensuring the clinical software strikes a proper balance between speed of access and surety as to the correct identity of the individual.	Accepted	The Department will incorporate this into the design parameters for the conformance requirements.
5.24	That the PCEHR System Operator use proactive monitoring of the use of exception-based searching for an IHI, to search for possible examples of misuse of the system.	Supported	The Department considers that monitoring of exception based searching for an IHI is appropriate, but that this is more properly conducted by the HI Service Operator, which would be privy to the searching.

No.	Recommendation	Response	Discussion
			The HI Service Operator currently has an obligation to maintain a record of all requests made to it for disclosure of an IHI (section 10, *Healthcare Identifiers Act 2010*). The PCEHR legislation will ensure that this obligation to applies to new disclosures of IHIs which the HI Service Operator may make in relation to the PCEHR system.
5.25	That the PCEHR System Operator use proactive monitoring of the audit logs of activity against the PCEHR of public figures, to search for possible examples of misuse of the system.	Accepted	The Department considers that this is a fundamental part of the monitoring framework required for the PCEHR system.
5.26	That the PCEHR Bill define the circumstances in which a consumer's access controls and other privacy settings may be overridden as only when the override is 'necessary to prevent or lessen a serious and imminent threat to the life or health of any consumer'.	Accepted	The PCEHR legislation is consistent with this recommendation (s64).
5.27	That the PCEHR System design ensure that access granted via the 'emergency access' override is only temporary.	Accepted	The PCEHR system design is consistent with this recommendation.
5.28	That users be provided with guidance on the interpretation of the legislative 'emergency access' test, with specific examples developed in consultation with the Australian Privacy Commissioner. This guidance should be clearly available whenever the 'emergency override' button is presented, for example by way of a link or pop-up box.	Supported	The Department agrees that there is a need for clear and practical guidance material about when ‘emergency access’ may be called upon, and that the Australian Privacy Commissioner is a key stakeholder who can provide valuable assistance in the development of this material.
5.29	That the data quality framework for the PCEHR System design should ensure that the only mandatory field for identity/demographic data in relation to clinical records is the consumer's IHI.	Not accepted	Demographic data in a record allows a healthcare provider to make sure they are looking at the PCEHR of the right consumer, and as a result giving appropriate treatment to them. A bare IHI does not assist healthcare providers to do this. The Department will, however, review the minimum mandatory dataset to make sure that there is not

No.	Recommendation	Response	Discussion
			superfluous demographic data being included in mandatory fields.
5.30	That the design makes it clear that the indigenous field status (as a type of 'sensitive personal information subject to special protection) is optional and not required to be completed.	Accepted	
5.31	That the conformance tests for clinical software to connect to the PCEHR System should include ensuring that no records are uploaded automatically from the local system to the PCEHR; that is a HPI-I user must make a 'manual' decision in relation to each upload.	Accepted	The current design reflects this. A record does not get sent to the PCEHR system unless the healthcare provider takes action (such as pressing a button) to send it.
5.32	That healthcare providers be provided with guidance on what records might not be appropriate to upload including where there are other legal restrictions in place.	Accepted	The Department recognises that healthcare providers are currently subject to State and Territory laws which impose confidentiality obligations on them (for example, in relation to reportable disease status, such as HIV infection). It is not intended that the PCEHR system override these obligations. The Department will develop communications material for providers which reminds them that they need to continue to observe secrecy or confidentiality obligations in their jurisdiction.
5.33	That the PCEHR Bill prohibit any disclosure of Consumer Notes except where the PCEHR System Operator is compelled to do so by way of a court order or similar.	Accepted in Principle	The PCEHR system is being designed so that only the consumer or their representative can view the consumer's notes which are identified as consumer only. The legislation provides that consumer only notes are only made available with the consent of the consumer (s66). They are not to be collected, used or disclosed by a participant in the PCEHR system, even in an emergency, or for the collection use or disclosure that is authorised by law or to a court or tribunal (s61, 64, 65, 69).

No.	Recommendation	Response	Discussion
5.34	That the PCEHR Bill define the extent to which the PCEHR System Operator will be considered to 'control' records held in Conformant Repositories but which are available through its indexing service, for the purposes of responding to a subpoena, warrant, notice to produce or other instrument.	Accepted	The PCEHR legislation will provide an express framework for the application of subpoenas, warrants and other kinds of notices to produce (s69). The principle underlying the design of the legislation is that the PCEHR system should be properly accountable to courts and tribunals for its own actions, but should not be required to produce consumers' information, unless it relates directly to the administration of the PCEHR system or to a coronial inquiry or indemnity cover for a provider. Where proceedings are about the administration of the PCEHR system, such as the prosecution of an offence, then the PCEHR operator can be required to release contents of a consumer's PCEHR to a court or tribunal, including parts of the PCEHR stored in repositories.
5.35	That the PCEHR Bill define the extent to which healthcare provider users of the system will be considered to 'control' any data held in or indexed through the PCEHR, for the purposes of responding to a subpoena, warrant, notice to produce or other instrument.	Accepted	The PCEHR legislation provides by implication that healthcare providers may not draw documents down from the PCEHR system for the purpose of responding to a subpoena, warrant or other kind of notice to produce. Any such requests must be handled through the System Operator.
5.36	That the PCEHR Bill prescribe whether the PCEHR System Operator can allow the disclosure, for research purposes, of records held in Conformant Repositories but which are available through its indexing service.	Accepted	The PCEHR legislation provides for information in the PCEHR system which identifies a person to only be available for research purposes with the consent of that person (s66). Accordingly, the access for research purposes to records held in a repository will be managed on that basis.
5.37	That the PCEHR Bill prescribe whether the PCEHR System Operator can allow the disclosure, for research purposes, of records which the consumer has sought to 'Remove from	Accepted	The PCEHR legislation allows research using information which identifies a person only with the consent of that person (s66).

No.	Recommendation	Response	Discussion
	View'.		Accordingly, the access for research purposes to records held in a repository will be managed on that basis.
5.38	That the PCEHR Bill include a note to the effect that the rules under which personal information may be disclosed by the PCEHR System Operator for research, for law enforcement purposes, or when obligated under a subpoena or similar instrument are to be found in the Privacy Act.	Accepted in principle	The current design of the PCEHR legislation sees these matters specifically dealt with within that legislation; there is no need for cross referencing to the Privacy Act to point users of the legislation to where to find these requirements.
5.39	That consumer communications (and in particular, the privacy notice provided at the time of registration) reflect the possibility that information from their PCEHR may be disclosed for research or law enforcement purposes, or when required by law, such as in response to a subpoena if the consumer is involved in litigation.	Accepted	The content and accessibility of privacy notices and other consumer communications is a priority for the Department.
6.1	That the PCEHR Bill ensure that child consumers aged 14 through 17 who seek to take control of their PCEHR have the right to do so, and that their rights include decisions to suspend or deactivate their record.	Accepted	This is reflected in the legislation (s6(3)). When in control of their record the consumer will have full rights to make decisions in relation to it.
6.2	That the PCEHR Bill set a data retention period for PCEHR records in the 'Active' category which have not been subject to any action on the record (such as any new data being added) for an extended period of time.	Accepted in part	The Department considers that it may be useful to include protocol for suspending a record after it has not been active for a specified period, but not that this is appropriate for inclusion in legislation. The Department will examine the feasibility of this recommendation from a technical perspective.
6.3	That the consumer communications about suspension and deactivation of records clarify that although documents held in Conformant Repositories may no longer be found through a suspended or deactivated PCEHR, they will be held by the Conformant Repositories and/or in local clinical systems for periods as determined by local data retention requirements.	Accepted	The Department agrees that consumer communications need to clearly explain privacy control settings to consumers, including their limitations.
6.4	That the exception for emergency access is clearly communicated to consumers prior to the PCEHR entering	Accepted	The Department agrees that consumer communications

No.	Recommendation	Response	Discussion
	'suspension mode'.		need to clearly explain privacy control settings to consumers, including their limitations.
7.1	That the PCEHR Bill ensure that the PCEHR System Operator is subject to the NPPs (or rules based on the NPPs) rather than the IPPs in the Privacy Act.	Accepted in principle	The Department is proposing that the PCEHR system operator is subject to specific privacy regime, which incorporates both the IPPs and NPPs. In particular, these privacy rules provide specific protection for health information, as occurs in the NPPs.
7.2	That the PCEHR Bill establish the PCEHR System Operator's authority to use and disclose data (including metadata) from a consumer's PCEHR for reporting purposes. The legislation should set out the bodies to whom personal information may or must be disclosed by the PCEHR System Operator including a reference to reporting obligations created in other legislation.	Accepted in principle	The PCEHR legislation allows for the sharing of information between the bodies delivering the PCEHR system services ('service delivery partners') to consumers and healthcare providers, for the purpose of management of the system. This sharing is to allow the service delivery partners to cooperate to ensure the system is working properly from a technical point of view, and to facilitate the identification and investigation of any misuse of the system (s63).
7.3	That the PCEHR System Operator ensure strict conformance requirements on HPI-Os to ensure users are uniquely identified to the System Operator at every login.	Accepted	The Department will include this in conformance requirements which healthcare provider organisations will be required to meet in order to intially connect, and maintain connection rights, to the PCEHR system.
7.4	That the PCEHR Bill establish the PCEHR System Operator's authority to use and disclose audit log data from a consumer's PCEHR for complaint-handling and law enforcement purposes. The legislation should set out the bodies to whom personal information may or must be disclosed by the System Operator, including the Australian Privacy Commissioner or other privacy regulator in the case of a privacy complaint, or to the appropriate law enforcement agency in the case of suspected unlawful use.	Accepted in principle	The Department agrees that there needs to be a framework around the use and disclosure of audit log information in the PCEHR system. The Department considers, however, that this framework needs to be principle based like existing privacy legislation, rather than naming specific organisations which may receive audit log data. The principle approach means that the information can be disclosed to the law enforcement agency which is appropriate to the circumstances of the case.

No.	Recommendation	Response	Discussion
7.5	That the PCEHR Bill establish the right of a consumer to obtain a copy of the summary version of their audit log through assisted channels, without charge.	Accepted in principle	The PCEHR system operator will be required to provide an individual with information about him or herself without charge in accordance with the requirements of existing Commonwealth Information Privacy Principles. The legislation also enshrines a right for an individual to their audit log and a summary or complete record of flows of their information (s15(1)(g) and (h)).
7.6	That prior to finalisation of operational plans for the PCEHR System Operator, there should be an assessment of the information security classification for data to be held by the PCEHR System Operator, and data when in transit to or from the PCEHR System Operator, and a corresponding independent Threat and Risk Assessment of the security controls proposed as a result.	Accepted	The Department will conduct a Threat and Risk Assessment.
7.7	That the Threat and Risk Assessment examine the adequacy of legislative or other protections against the risk of exposure of consumers' personal information to foreign law enforcement bodies.	Accepted	The Department will consider this as part of the Threat and Risk Assessment.
7.8	That the Threat and Risk Assessment be reviewed by the Department's privacy team in conjunction with this and any other PIA reports.	Accepted	The Department considers that this is a sensible approach.
8.1	That the PCEHR Bill include a set of 'PCEHR privacy rules' governing all non-consumer users of the PCEHR System, which should encompass: (1) authorised purposes for searching for or 'viewing' information from a PCEHR; (2) authorised purposes for copying or 'downloading' information from a PCEHR; (3) authorised purposes for using information from a PCEHR (whether or not it has been copied or downloaded first); (4) authorised purposes for adding or 'uploading' information to a PCEHR;	Accepted	The PCEHR legislation provides for comprehensive arrangements to protect the privacy of the consumer information in the PCEHR. The legislation sets out the authorisation for collection use and disclosure of a consumers PCEHR information which cover accessing, viewing, copying or downloading for providing healthcare (s61-70). It provides that activities not covered in these provisions are unauthorised (s59), as well as secondary uses where the obtaining of the

No.	Recommendation	Response	Discussion
	(5) obligations to take reasonable steps to protect the data security of the PCEHR; and (6) obligations to take reasonable steps to ensure the data quality of information added or 'uploaded' to the PCEHR. **Note**: We have used the term 'privacy rules' here simply to distinguish our proposal from existing privacy principles'. Terms such as 'privacy protocol' or 'privacy standards' may be equally appropriate.		information was not authorised (s60). More particular obligations to protect the security of records are able to be set out in rules or in regulations (s109, 112).
8.2	That the 'PCEHR privacy rules' incorporate an enforcement mechanism which provides that a contravention of those rules is an 'interference with privacy' under the federal Privacy Act - and, if the contravening conduct was intentional, also a criminal offence.	Accepted in part	The PCEHR legislation makes a breach of PCEHR privacy rules a breach of the Privacy Act (s73), and includes civil penalties for intentional privacy breaches, (s59, 74-78). The PCEHR system will operate in a legal framework which already includes a range of criminal offences applying to misuse of computers, data, telecommunications services and healthcare identifiers. These will automatically apply, irrespective of the new penalties created by the PCEHR legislation. For example, part 10.7 of the Commonwealth Criminal Code lists cybercrime offences which criminalise the use of computer systems to carry out cyber attacks. The penalties for these offences range from two to 10 years imprisonment. The offences in Part 10.7 include: • Section 477.1: *Unauthorised access, modification or impairment with intent to commit a serious offence* – unauthorised use of computer technology to commit serious crimes. • Section 477.2: *Unauthorised modification of data to cause impairment* – the unauthorised modification of data on a computer that would impair access to, or the reliability, security or operation of the data. For example, this offence would cover a person who uses the internet to infect a computer with malware. • Section 477.3: *Unauthorised impairment of electronic*

No.	Recommendation	Response	Discussion
			communication – cyber attacks such as denial of service attacks, where a server is inundated with a large volume of data intended to impede or prevent its functioning. • Section 478.1: *Unauthorised access to, or modification of, restricted data* – unauthorised access to, or modification of, data held on a computer that is restricted by an access control system. For example, this offence would cover hacking into password protected data. • Section 478.3: *Possession or control of data with intent to commit a computer offence* – people who possess programs designed to hack into other people's computer systems or impair data or electronic communications. For example, this offence covers possessing a program which will enable the offender to launch a denial of service attack against an Australian Government agency's computer system. • Section 478.4: *Producing, supplying or obtaining data with intent to commit a computer offence* – the production and/or supply of data to be used in a computer offence. This offence would cover people who trade botnets and malware. The PCEHR legislation provides the ability to make criminal offences using a regulations power. The penalties in the principal legislation, however, are civil in nature. Civil penalties have been chosen rather than criminal because there is a lower standard of proof required to convict a person of a civil offence. With imposition of a civil penalty being more likely, the Department considers that this both encourages enforcement of penalties by the PCEHR system operator, and acts as a significant deterrent to misuse.

No.	Recommendation	Response	Discussion
8.3	That the 'PCEHR privacy rules' cover conduct relating to information gained from a PCEHR by an authorised user of a PCEHR. The scope of regulated conduct should not be limited to conduct done 'in the performance of their duties' (cf s 8(1) of the Privacy Act), and there should be no exception allowing use of the information gained from a PCEHR for 'personal, family or household affairs' (cf s 26(2)(c) of the HI Act). That is, the obligations must extend to the misuse of information by a 'rogue' employee, agent or contractor, who uses or discloses information from a PCEHR for their own, unauthorised purposes. The obligations must also extend to the recipient of information gained from a PCEHR by an authorised user of a PCEHR, so as to ensure that it is an offence for a third party to use or disclose information from a PCEHR which was improperly obtained	Accepted	The PCEHR legislation is consistent with this recommendation (s59-60).
8.4	That the 'PCEHR privacy rules' provide that in the case of an alleged contravention, the respondent to a complaint to the Privacy Commissioner shall be the employing organisation, rather than the individual employee, agent or contractor (see s 8(1) of the Privacy Act).	Accepted	The PCEHR legislation is consistent with the application of section 8(1) of the Privacy Act to agencies and organisations participating in the PCEHR system (eg s93). Individuals will be liable for specific civil penalties under the PCEHR legislation, however, if they engage in deliberate misuse of the PCEHR system or information within it, where this is not within the actual or apparent scope of their employment.
8.5	That the criminal penalties for intentional contravention of a 'PCEHR privacy rule' should be as per s 26(1) of the HI Act, namely a maximum two years imprisonment and/or 120 penalty units. Criminal penalties may be applicable to an individual employee, agent or contractor, or to a corporate person.	Accepted in part	The PCEHR system will operate in a legal framework which already includes a range of criminal offences applying to misuse of computers, data, telecommunications services and healthcare identifiers (see 8.2 for details). These will automatically apply, irrespective of any new penalties created by the PCEHR legislation. The penalties in the principal legislation are civil in nature. Civil penalties have been chosen rather than criminal because there is a lower standard of proof required to

No.	Recommendation	Response	Discussion
			convict a person of a civil offence. With imposition of a civil penalty being more likely, the Department considers that this both encourages enforcement of penalties by the PCEHR system operator, and acts as a significant deterrent to misuse. The legislation provides for the regulations to set out criminal penalties in respect of offences against the regulations (s112).
8.6	That the PCEHR Bill authorise healthcare providers to disclose personal information and health information to a PCEHR, such as to authorise non-compliance with NSW HPP 14 and 15, Vic HPP 9, Tas PIPP 9 and NT IPP 9.	Accepted	The Department agrees that express authorisation in the PCEHR legislation may be required to allow healthcare providers in some States and Territories to participate in the PCEHR system. The legislation is designed to overcome the effect of any state or territory law that would prohibit or restrict uploading information to the PCEHR (s41). The legislation also provides for any limitation in a state or territory law to be preserved where this is considered appropriate by having the law prescribed in regulations(s41).
8.7	That when the draft forms and terms and conditions (versions relating to each of the access channels) are completed, the forms and terms and conditions be reviewed for IPP/NPP compliance.	Accepted	The Department will engage in an ongoing program of privacy review as the design is refined and built.
8.8	That the PCEHR Bill provide for a complaint-handling process with clear time limits and pathways, which commences with the PCEHR System Operator and can then be escalated, by either the complainant or the PCEHR System Operator, to the Australian Privacy Commissioner.	Accepted in part	Under the legislation, one of the functions of the System Operator is to provide national arrangements for consumers and participants to make complaints relating to the PCEHR system, although consumers will still have the ability to lodge complaints with other appropriate bodies such as national or state privacy or health information regulators (s15(1)(j)).

No.	Recommendation	Response	Discussion
			The Department considers that it is important for a complaint handling process with clear time limits and pathways, but does not consider that the principal legislation is the best place for these to be specified. Because a complainant may have the ability to make a complaint in more than one jurisdiction about the same handling of information, there may be limitations on the Commonwealth's ability to act unilaterally in this space. As a result, the Department considers that memoranda of understanding or other similar arrangements are better suited to this purpose.
8.9	That the PCEHR Bill not exclude complainants from lodging a complaint or seeking a remedy in any other forum	Accepted in principle	The Department supports the ability of a consumer to pick the forum of his or her choice to pursue a privacy complaint. The Department will, however, be seeking to design its complaints mechanism in a way which does not allow for 'double dipping'; that is, if a consumer has pursued a complaint to resolution in one forum, there should not be an ability to reopen the matter in another.
8.10	That the PCEHR Bill include an obligation on the PCEHR System Operator to report any data security breaches and any evidence of internal misuse of PCEHR data to the Australian Privacy Commissioner.	Accepted	The PCEHR legislation provides for reporting of data breaches (s75). Where the Service Operator is involved it is required to notify the Australian Information Commissioner and all affected consumers (s75(4).
8.11	That the PCEHR Bill provide the PCEHR System Operator with the power to disconnect or revoke the access of an authorised representative, ARA, CPP, CRP or HPI-O; or to compel an HPI-O to disconnect or revoke the access of a specific user.	Accepted	The PCEHR legislation provides the PCEHR system operator with the ability to suspend, terminate or impose conditions on the right of other system participants to connect to the system (s51-54). These conditions can extend to requirements about access to the system by employees of the system participant. Details of requirements can be included in the Rules.

No.	Recommendation	Response	Discussion
8.12	That the PCEHR Bill provide the Australian Privacy Commissioner with the power to compel the PCEHR System Operator to exercise its power to disconnect or revoke the access of an individual or organisation	Not accepted but seek the Senate Committee's views	The PCEHR legislation does not give powers to the Australian Information Commissioner to instruct the PCEHR system operator if and when to exercise its powers. The Department considers that there are a range of other mechanisms in the legislation which will support the same outcome, being the use of remedial powers where appropriate to ensure the integrity of the PCEHR system. Those mechanisms include: ▪ The PCEHR system operator will be accountable to the Parliament for the level of its monitoring, investigation and enforcement activities through annual reporting obligations (s107); and ▪ The Australian Information Commissioner will have significant powers of his own, relating to privacy breaches, offences under the PCEHR legislation, enforceable undertakings, injunctions and also be accountable to Parliament through annual reporting obligations (s73, 79, 94, 96, 106).
8.13	That the Department encourage State and Territory governments to ensure legislation or protocols allow some flexibility in the application of time limits in their jurisdictions, so that their time limits do not start to 'run' until the Australian Privacy Commissioner has advised a complainant of their option to lodge their complaint in that other jurisdiction.	Accepted in principle	The Department will raise this issue for consideration with its counterparts in the States and Territories. There will need to be an analysis of what measures might be required to support this.
8.14	That the Australian Privacy Commissioner to be adequately resourced to manage any additional workload expected to arise from implementation of the PCEHR System	Accepted	Funding proposals for the PCEHR system will include provision for regulatory activity as a matter of course.
8.15	That consumer communications clearly articulate to consumers their privacy 'rights', the privacy 'rules' which	Accepted	The Department agrees that these are fundamental

No.	Recommendation	Response	Discussion
	participants in the PCEHR System must follow, and the complaint-handling process.		components to be included in consumer communications.
8.16	That the PCEHR Bill include an obligation on ARAs, CPPs, CRPs and HPI-Os to report any data security breaches, and any evidence of internal misuse of PCEHR data, to the Australian Privacy Commissioner and the PCEHR System Operator.	Accepted	The PCEHR legislation provides for reporting of data breaches (s75).
8.17	That a Threat and Risk Assessment examine the adequacy of legislative or other protections against the risk of exposure of consumers' personal information, held by ARAs, CPPs, CRPs and HPI Os, to foreign law enforcement bodies.	Accepted	This will be one component of the Threat and Risk Assessment which will be conducted of the system.
8.18	That prior to completion of the operational level design of the PCEHR System and prior to the PCEHR System entering the 'live production' environment, the Department commission further privacy reviews of: (11) the draft operational level design; and (12) the draft consumer communications and terms & conditions, to be developed by the Change and Adoption Partner.	Accepted	The Department will have an ongoing program of privacy review of all aspects of the program.
8.19	That the PCEHR System include an on-going oversight and governance committee, including representation from the Privacy Officer of the Department as well as State and Territory bodies, to manage the following functions: (1) promote and report on privacy compliance; (2) review any requests to change the audit logging regime or data security controls applying to the PCEHR System; (3) review and commission PIAs for: (a) any proposal to enhance, expand or amend the scope of the data to be held in, or indexed through, the PCEHR; and (b) any proposal to enhance, expand or amend the scope of the PCEHR System as a whole; (4) commission regular privacy audits and information security audits of the PCEHR System; (5) review privacy complaints arising from use of the PCEHR	Accepted in principle	The Department will put in place a formal governance structure to monitor and evaluate privacy compliance and management within the PCEHR system. The kinds of stakeholders and activities identified in the PIA accord with the general principles which the Department will use to develop the framework.

No.	Recommendation	Response	Discussion
	System; and (6) update staff training and user manuals as needs be.		
8.20	That this PIA Report be provided to the Australian Privacy Commissioner and all State/Territory Privacy Commissioners or equivalent regulators.	Accepted	
8.21	That this PIA Report be published online by the Department, together with the Department's response to the recommendation	Accepted	

PHASE 2 RECOMMENDATIONS

9.1	Make it clear whether the authorised representative is required to have a verified healthcare identifier (4.7.6(a))	Accepted	Ordinarily a verified individual healthcare identifier will be required. The PCEHR legislation supports this as a general requirement, but also provides for the PCEHR Rules to specify where a verified healthcare identifier is not required (s6(6)). As explained in the explanatory memorandum, it is envisaged that such PCEHR Rules would be made in only limited circumstances. For example, where a child is under the guardianship of a statutory office holder such as a public guardian, it is not intended that the statutory office holder or their staff would use their own healthcare identifier to identify themselves to the System Operator when acting as an authorised of the child. However, it is important that such people are identified and paragraph 6(6)(b) will permit PCEHR Rules to be made for this purpose
9.2	The PCEHR Rules should accommodate concurrent access to the PCEHR by the consumer and authorised representative (4.7.6(b)).	Accepted	The PCEHR legislation provides that a consumer may set the access controls for a nominated representative. A consumer may agree to their nominated representative having concurrent access to the PCEHR record and the

			same right to control the record that they have and can exercise those rights at the same time as the consumer (s7).
9.3	Make it clear that the PCEHR Rules will specify the default access controls (4.9.4) and the consumer's ability to correct errors in the PCEHR (5.1.10(a)).	Accepted	The PCEHR legislation provides for default access controls to be specified in the PCEHR rules (s109(3)(e)). It is intended that any errors in a record will be able to be corrected through the provider responsible for the uploading if the information. The Service Operator is required to ensure that the system is administered so that problems relating to the administration of the system can be resolved (s15(1)(k)). Rules may be made on requirements for administration and day to day operations (s109(3)).
9.4	Make it clear that information is uploaded as a feature of the PCEHR System unless a consumer advises otherwise (5.6.9).	Accepted	The PCEHR legislation provides that information is to be uploaded to a PCEHR record by a healthcare provider unless the consumer advises that it should not (s45(d)).
9.5	Make it clear that healthcare providers must comply with a request by a consumer that a document should not be uploaded (5.6.10).	Accepted	The PCEHR legislation provides that information is to be uploaded to a PCEHR record by a healthcare provider unless the consumer advises that it should not (s45(d)).
9.6	Make it clear that the System Operator can only use information obtained under s 44 in accordance with its functions. In addition it would be useful for the explanatory memorandum to provide examples of what such uses may be (5.7.9(f)	Accepted	The information provided under s50 can only be used by the Service Operator in accordance with a function that they have, such as to those set out in Division 4 of Part 2. The explanatory memorandum includes an example of an emergency situation under s64.
9.7	Make it clear that the PCEHR Rules should specify the nature of the information to be included in the register (5.7.9(g)).	Accepted	The PCEHR legislation provides for administrative information to be included in the Register and already provides for the Rules to specify information (s57). To make it clearer, the Explanatory Memorandum notes that the administrative information may include personal

			information, for example name and address.
9.8	Ensure that the enforcement regime that applies to the System Operator for a breach of the Bill (whether through the Bill and/or other laws) is as effective as the enforcement regime that will apply to other participants who breach the Bill(8.2.8(e)).	Accepted	The Department is satisfied that the enforcement regime is equally as effective against the Service operator as other participants. The Service Operator is legally bound to comply with the requirements set out in the legislation, as are participants who are Government bodies. As noted in the explanatory memorandum, there are a range of remedies and accountabilities that apply against the Service Operator. It may be subject to a declaration or injunction, investigated by the Information Commissioner under the Privacy Act, investigated by the Ombudsman, subject to Parliamentary scrutiny or subject to claims for breach of statutory duty. While the Crown may have immunity in certain regards, the employees and contractors of the Crown will not necessarily have any such immunity. Also, nothing in the Bill prevents an individual who suffers loss or damage from seeking to recover that loss or damage from the person who caused it. The PCEHR legislation includes a note to make clear that while the Crown is not liable to be prosecuted for an offence or liable for a pecuniary penalty, other rights and remedies available against Government agencies involved as participants in the PCEHR system will continue to apply (s11).
9.9	The Explanatory Memorandum describe the alternative remedies available under concurrent legislation and common law (such as breach of confidence) (8.2.8(f)).	Accepted	The power of the Australian Information Commissioner is not limited to the enforcement regime under the Privacy Act, the PCEHR legislation provides additional powers. The explanatory memorandum describes the range of remedies that are available. Action under a state or territory privacy regime is not precluded nor is an

			individual's right to take action to recover the loss or damage from the person who caused it (see explanatory memorandum comments against s11).
9.10	The System Operator should be required to refer to the OAIC's Guide to Handling Personal Information Security Breaches when considering whether to notify a consumer of a breach of data (8.2.8(n))	Accepted	The PCEHR legislation has been amended to remove any discretion on the part of the Service Operator. This is a higher standard than under the OAIC's guidelines which apply only where there is a serious breach. Where the Service Operator is involved it is required to notify the Australian Information Commissioner and all affected, as well as the general public if a significant number of consumers are affected (s75(4)). The other requirements set out in the legislation reflect relevant factors described in the OAIC guide. It is not considered appropriate that having regard to the guide, should be fixed in the principal legislation but it is expected that as a matter of administration the guide would be referred to as a matter of course.