Response to Request for Comment

on the Personally Controlled Electronic Health Record (PCEHR) System: Legislation Issues Paper

August 2011

Authored by Fellows and Members of the

Australasian College of Health Informatics

PO Box 125, GLEN IRIS 3145, Australia Secretary@ACHI.org.au www.ACHI.org.au

Index

Executive Summary

The Australasian College of Health Informatics (ACHI) welcomes this opportunity to comment on the "Personally Controlled Electronic Health Record (PCEHR) System: Legislation issues paper" released by the Department of Health and Ageing on 6 July 2011.

The College is the professional body for Health Informatics in the Asia-Pacific Region. The credentialed Fellows and Members of the College are national and international experts, thought leaders and trusted advisers in Health Informatics. ACHI sets standards for education and professional practice in Health Informatics, supports initiatives, facilitates collaboration and mentors the community. The Fellows and Members of the College are widely involved in e-Health research, standards development, system design and implementation work in Australia, the region and globally.

ACHI supports the Australian government's national health reform agenda as informed by the National Health and Hospitals Reform Commission, the Primary Health Care Reform Report and the National Preventative Health Strategy Roadmap. We welcome an agenda that aims to create an improved healthcare system that is safe, of high quality and which is transparent, accountable, affordable and sustainable.

The College agrees that e-Health is an important enabler to the way healthcare will be delivered in the future. The College is supportive of robust privacy legislation as this is considered to be an important foundation to progress e-Health. We recognise the need to consider the introduction of separate PCEHR legislation where existing privacy and health legislation is inadequate or does not cover the specific privacy issues associated with the introduction and ongoing operation of the PCEHR. The College believes that it is necessary that any required legislative changes (including the introduction of PCEHR specific legislation or amendments to existing Commonwealth and State legislation or regulations) properly address the privacy concerns and community perceptions of a lack of adequate security of personal health information in addition to the privacy and governance issues raised by the Australian Privacy Commissioner[1] and the Australian Privacy Foundation[2] in their review of the PCHER ConOps draft documentation and submissions to DOHA.

The College believes that specific PCEHR privacy legislation which may be required to support the implementation and operational use of the PCEHR system should:

a. be fully in alignment and consistent with,

b. not negatively impact, and

c. appropriately complement

the privacy rights of individuals and the protection of personal information specified under existing Commonwealth and State Privacy, Health and other relevant legislation and regulations which constitutes the current privacy framework in Australia.

---

[1] Australian Privacy Commissioner: Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system. Submission to DOHA June 2011. http://www.oaic.gov.au/publications/submissions/2011-06%20Submission%20on%20PCEHR%20ConOps%20FINAL.html

[2] Australian Privacy Foundation: APF Feedback about the Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system. 30 May 2011.
http://www.yourhealth.gov.au/internet/yourhealth/blog.nsf/D17E15298A0C84E8CA2578DA0005BA7F/$FILE/Australian%20Privacy%20Foundation%20submission.pdf

Addendum to the APF Feedback about the Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system. (30 May 2011) – 5 June 2011.
http://www.yourhealth.gov.au/internet/yourhealth/blog.nsf/D17E15298A0C84E8CA2578DA0005BA7F/$FILE/Australian%20Privacy%20Foundation%20submission%20addendum.pdf

Therefore, the College welcomes the Department's release of the "Personally Controlled Electronic Health Record (PCEHR) System: Legislation issues paper" for public comment. The Fellows and Members of the College have reviewed the draft and have identified a number of issues of concern, which require further clarification and due consideration.

In summary, the legislation issue paper covers most of the aspects that ACHI believes are relevant. However, there are a number of areas where the College believes substantial clarifications and improvements are required and has formulated **42 recommendations** for the Department's consideration:

Recommendation 1: *That the PCEHR legislation address the issues of record completeness, accuracy, provenance and timeliness.*

Recommendation 2: *That the Department consider the medico-legal implications of clinicians' responsibility for appropriateness and completeness of the PCEHR.*

Recommendation 3: *That the PCEHR legislation address the issues potentially created by the use of personal computing devices to access the PCEHR.*

Recommendation 4: *That the Department ensure that the PCEHR legislation is consistent with all other legislation, regulations and legal processes.*

Recommendation 5: *That the Department, when drafting the PCEHR legislation include the following participants:*

1. *Government jurisdictions / agencies (including the recipients of health data, reports and those organisations that may seek or require authorised secondary use of health data for epidemiology, population health and clinical research purposes)*
2. *Audit provider(s) for audit of operational management, security, access control etc*
3. *Complaints management provider*
4. *Consumer registration organisations (and associated certification organisations)*

Recommendation 6: *That the Department consider the findings from the NEHTA Security and Access Framework showing that Individual Health Identifiers are not safe for the purpose of uniquely identifying[3]. In our experience, patient identification processes are more effective when they rely on other forms of identification, such as address and/or phone number as well as an IHI or UR.*

Recommendation 7: *That the legislation address the possibility of unauthorised access to PCEHR information though inappropriate search algorithms.*

Recommendation 8: *That the Legislation not limit the use of non-health organisations as registration authorities provided they are certified by an independent authorised certification body / organisation.*

Recommendation 9: *That the PCEHR legislation include the roles and responsibilities of both bodies (registration and certification organisations) and other criteria that these bodies would need to comply with (including compliance with the Privacy Act and requirement to be bound by Australian law).*

[3] Security and Access Framework http://www.nehta.gov.au/component/docman/doc_download/877-security-and-access-framework

Recommendation 10: *That the PCEHR legislation include the option of non-physical identification artefacts for enrolment.*

Recommendation 11: *That the Department consider when drafting legislation that some patients change their minds frequently and may wish to change authorised representatives once or more per year. The PCEHR system operator will need to audit the changes to mitigate risks that might be associated with often-changed authorised representatives.*

Recommendation 12: *That the Department consider cases where a minor is responsible for their own PCEHR in the same way as those 18 years and over.*

Recommendation 13: *That the following obligations to be required of the PCEHR system operator:*

1. The PCEHR operator should be:
   a. a Legal Entity in Australia;
   b. an entity that is fully independent of Government, PCEHR performance assessment and audit bodies. The PCEHR operator may be a private sector business, a NGO or statutory body); and
   c. subject to privacy obligations under Australian law (including the Privacy Act)
2. Service Levels / Performance requirements should be broadly covered in the PCEHR legislation (as high level objectives and targets), however detailed performance and service level requirements (including detailed metrics/ measures to be used, how they will be assessed and penalties for not meeting targets etc) should be included as part of the contract and service level agreement with the PCEHR operator - the performance and service level information should be published and made available to the public online (via website)
3. Directors of the System Operator must be subject to Australian law.

Recommendation 14: *That the PCEHR legislation include the requirement that repository operators be subject to privacy obligations under Australian law (including the Privacy Act).*

Recommendation 15: *That the roles and responsibilities of Repository operators be specified in the PCEHR legislation.*

Recommendation 16: *That the repository operators be subject to Australian law (including the Privacy Act).*

Recommendation 17: *That the repository operators require certification in accordance with certification criteria specified in the PCEHR legislation.*

Recommendation 18: *That future addition of trusted data sources should require formal amendment of the PCEHR legislation.*

Recommendation 19: *That no other "trusted" data sources be considered at this stage. Any future additions of "trusted" data sources needs to be made by amendment of the PCEHR legislation and not through regulations (this is important since amendment of regulations would allow social security, passport / immigration, tax and financial information data sources to be very easily included at a future time).*

Recommendation 20: *That the legislation provide both a definition of and purpose of using a "trusted data source" and specify how it will be used by the PCEHR system and its operator(s).*

Recommendation 21: *That the roles and responsibilities of Portal providers be specified in the PCEHR legislation.*

Recommendation 22: *That the Portal providers be subject to Australian law (including the Privacy Act).*

Recommendation 23: *That the Portal providers require certification in accordance with certification criteria specified in the PCEHR legislation.*

Recommendation 24: *That all demographic or other personal information captured or used for PCEHR system purposes must be held in Australia.*

Recommendation 25: *That the Department consider the legislative issues raised by permanent archival or data migration to a different system if the PCEHR system is decommissioned in the future or if the individual wishes to cease using their PCEHR.*

Recommendation 26: *That the Department consider the legislative issues raised by patients requesting to have their record deleted or transferred to another.*

Recommendation 27: *That the legislation require that a comprehensive audit trail of all PCEHR activity / transactions related to changes made, information provided / uploaded, information accessed / downloaded or changes made relating to access control settings, or any other update of the record made by individuals, authorised or nominated representatives should be kept and be easily retrievable for review.*

Recommendation 28: *That the ability to choose a minor as the nominated representative be aligned and consistent with Medicare requirements regulations and specified in the PCEHR legislation.*

Recommendation 29: *That the Department consider training environments for operations and management of the PCEHR.*

Recommendation 30: *That the PCEHR operator (and its sub-contractors) and all providers (including health and ICT providers, portal and repository operators) and organisations / agencies / entities that use, maintain, operate or provide data or services to the PCEHR system (as part of its normal operations, support maintenance or enhancement) should be subject to the Privacy Act and privacy obligations under Australian law.*

Recommendation 31: *That personal information uploaded by individuals or PCEHR authorised health providers should be subject to the Privacy Act and privacy obligations under Australian law.*

Recommendation 32: *That the PCEHR legislation specifically refer to the requirements to protect the secondary uses and disclosure of personal information permitted under the Privacy Act.*

Recommendation 33: *That the PCEHR legislation specifically address the secondary use of pseudonymous personal health information for the purposes of epidemiology, population health and research purposes. This should include:*

a. *the criteria, constraints and limitations for authorised secondary use*
b. *the requirement for consent from the individual to 'opt-in' to allow access to this information,*
c. *the mechanism of pseudonymisation of personal health information to be employed*
d. *the legal requirements and obligations of authorised secondary users of PCEHR personal health information*

e. the requirements and process of registration of authorised secondary users of PCEHR personal health information, and

f. the penalties that would apply for inappropriate use or disclosure of this information

Recommendation 34: *That the PCEHR systems be required to implement robust data encryption technologies to electronically protect all Personal Information (PI) that is stored or electronically transmitted or exchanged with other authorised systems. The data encryption technology used to encrypt PI stored in the PCEHR system and all its datastores and repositories should be compliant with the Advanced Encryption Standard (AES) as certified by the National Institute of Standards Technology (NIST) or an equivalent or more secure data encryption standard as certified by NIST.*

Recommendation 35: *That all agencies (including Commonwealth, State government or NGOs), private sector organisations and individuals (i.e. not just healthcare providers and organisations) that are permitted access to PCEHR systems or PCEHR information stored in repositories or datastores (e.g. for the purpose of system administration, operation, research or any other authorised purpose) should at a minimum comply with privacy, security and confidentiality requirements as specified in existing commonwealth and state privacy and health record legislation.*

Recommendation 36: *That specific PCEHR legislation should include specification of the purposes for which authorised access to the PCEHR systems and data will be granted, administered, monitored and how privacy and security breaches will be dealt with (i.e. enforcement, penalties etc.)*

Recommendation 37: *That the Department consider more severe penalties (including imprisonment) for unauthorised PCEHR access by organisations or individuals acting for organisations.*

Recommendation 38: *That the legislation include provisions for penalties (including imprisonment) for any negligent and/or intentional acts by repository or portal operators that result in PCEHR privacy breaches.*

Recommendation 39: *That the PCEHR legislation be abundantly clear and unambiguous regarding confidentiality obligations of all parties involved in the PCEHR.*

Recommendation 40: *That the Department ensure a gap analysis is undertaken regarding any differences in PCEHR disciplinary measures between government agencies and private operators.*

Recommendation 41: *That the Governance framework be referred to in the PCEHR legislation and:*

a. provide a high level of transparency and accountability

b. include engagement of the critically necessary stakeholder communities

c. provide a comprehensive list of all governance bodies and entities, inter-relationships between the entities, lines of reporting and authority, detailed roles and responsibilities, process for constituting and establishing governance entities, list of constituents of the governance entities, schedule of meetings of governance entities

d. reports, meeting agendas, minutes and other documentation to be made accessible to the public online (via a publicly accessible website) for review

e. mechanism for registering governance related issues or complaints online via a publicly accessible website that will be addressed by the appropriate governance entity (with communication of the issue status, any actions taken and final outcome from the appropriate governance entity to the person or organisation registering the issue)

f. detail any legal requirements of the various governance bodies or entities described under the PCEHR Governance arrangements that may be specified in the proposed PCEHR legislation, in particular with regard to the roles and responsibilities of relevant agencies and organisations authorised to perform or assist with the following:

i. design, develop, implement, maintain, support, operate, monitor, audit or assess the performance of the PCEHR system (including access to the system and PCEHR information);

ii. investigate alleged criminal activity or breach associated with operation, access to, or management of the PCEHR system; or

iii. investigate complaints from individuals (or authorised or nominated persons) or health providers relating to PCEHR access (and controls), record creation, population of the records, record content or unauthorised use or misuse of PCEHR information.

Recommendation 42: *That an Ombudsman-like body be set up to handle PCEHR complaints.*

The Australasian College of Health Informatics looks forward to further working with DoHA on the draft legislation to support the creation and usage of PCEHR e-health systems that will enable the common goal of better healthcare for all Australians.

Section 1.2 Introduction: What is not in scope

Although Section 1.2 places the Personally Controlled Electronic Health Record (PCEHR) system itself out of scope, the College wishes to outline some important contextual concerns and offer resulting recommendations:

a. Our core concerns are that the PCEHR is trying to bridge the divide between a Personal Health Record (PHR) and a Shared Electronic Health Record (SEHR). The Legislative Issues Paper and the "PCEHR Draft Concept of Operations" ("ConOps") suggests that the PCEHR system is considered as a PHR in the first instance and a SEHR second. Clinicians are on record stating that they will not rely upon a PHR for patient care.[4] To avoid repeating the unsatisfactory UK Summary Care Record experience[5], the College[6] and many other commentators[7] have suggested a change of approach is necessary. This changed approach would be emphasis e the importance of establishing a PHR as the primary focus if we are to meet the July 2012 deadline, while SEHR implementation may occur as a Public/Private partnership project in the future.

b. The College has expressed concern about the implications of Personal Control and the additional GP workflow burden the PCEHR system operation implies[8].

c. Data entry requiring human curation raises important questions about record completeness, accuracy, provenance and timeliness. The legislation supporting the introduction of the PCEHR system should address these questions.

> ***Recommendation 1:*** *That the PCEHR legislation address the issues of record completeness, accuracy, provenance and timeliness.*

d. The Legislative Issues Paper and the ConOps seem to hold clinicians to account for ensuring data on the Shared Health Summary record is 'appropriate' and up to date for patient care. The medico-legal implications of such needs exploration in the Legislative Issues Paper.

> ***Recommendation 2:*** *That the Department consider the medico-legal implications of clinicians' responsibility for appropriateness and completeness of the PCEHR.*

e. The Legislative Issues Paper needs to address important questions about the application of personal computing devices (eg tablets, smart phones, etc.) to the PCEHR system, especially in clinical settings. The college is aware that these devices are increasingly being used[9] and that many institutions are rapidly adopting a "BYO Computing" approach[10] [11].

> ***Recommendation 3:*** *That the PCEHR legislation address the issues potentially created by the use of personal computing devices to access the PCEHR.*

---

[4] RACGP Position Statement: Personally Controlled Electronic Health Record (PCEHR)", 27 July 2011, www.racgp.org.au/AM/Template.cfm?Section=ehealthPCEHR&Template=/CM/ContentDisplay.cfm&ContentID=43401

[5] Wright, O. "NHS pulls the plug on its £11bn IT system." The Independent, 3 August 2011. http://www.independent.co.uk/life-style/health-and-families/health-news/nhs-pulls-the-plug-on-its-11bn-it-system-2330906.html

[6] ACHI, "Comments on NEHTA PCEHR - Key Points Concept of Operations", unpublished, July 2011

[7] Greenhalgh T, Stramer K, Bratan T, Byrne E, Russell J, Hinder S, Potts H. The Devil's in the Detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace programmes. London: University College London; 2010.

[8] ACHI, Response to PCEHR Draft Concept of Operations, June 2011, www.achi.org.au/docs/ACHI_Response-PCEHR_ConOps_V1.2.pdf

[9] See www.informationweek.com/news/healthcare/EMR/228800929

[10] www.cio.com.au/article/391530/cios_lost_battle_against_bring_your_own_technology_/

[11] www.cio.com.au/article/393904/anz_deploy_ipads_following_due_process_weatherston

f. The Legislative Issues Paper and ConOps are unclear about whether an individual may build a consolidated view of their health summary (uncurated or self-curated) over time without relying on the PCEHR shared health summary.

g. Tensions between patient and GP influencing ongoing "trust" relationships[12]

h. The legislation must be enacted so that the entire community may rely upon it as, according to the Federal Court, does **no**t seem to have occurred in PSR rulings from 2005 onwards[13].

Recommendation 4: *That the Department ensure that the PCEHR legislation is consistent with all other legislation, regulations and legal processes.*

[12] Recommendation #xx, Response to PCEHR Draft Concept of Operations, ACHI, June 2011,

[13] Staff writers, Federal court rules PSR invalid. Medical Observer. Friday July 29. http://www.medicalobserver.com.au/news/federal-court--rules-psr-invalid

Comments on Questions and Proposals

Q1. Are there other potential participants in the PCEHR system and what is their role?

Recommendation 5: *That the Department, when drafting the PCEHR legislation include the following participants:*

1. *Government jurisdictions / agencies (including the recipients of health data, reports and those organisations that may seek or require authorised secondary use of health data for epidemiology, population health and clinical research purposes)*
2. *Audit provider(s) for audit of operational management, security, access control etc*
3. *Complaints management providers*
4. *Consumer registration organisations (and associated certification organisations)*

NOTE: The IT industry is too generic in this context. The list of participants should include PCEHR software providers only. Also there is no need to include infrastructure providers to the PCEHR operator as these should be managed through legally binding contracts (as sub-contractors) that specify obligations consistent with what is required under legislation for the PCEHR operator

Proposal 1: Legislation would specify that an individual would be entitled to be registered for a PCEHR if:

• he or she has a verified IHI; or

• in the case of individuals under 12 months who do not have a verified IHI, he or she has an unverified IHI; and

• the identifying information has been provided to enable registration.

Proposal 2: Legislation would enable the information flows necessary to verify the identity of individuals, and to create legally recognised rights and responsibilities for individuals.

Recommendation 6: *That the Department consider the findings from the NEHTA Security and Access Framework showing that Individual Health Identifiers are not safe for the purpose of uniquely identifying*[14]*. In our experience, patient identification processes are more effective when they rely on other forms of identification, such as address and/or phone number as well as an IHI or UR.*

ACHI is concerned about the algorithms used to search local administrative identification indexes by health professionals. These were designed for the patient and not the PCEHR system; they display all Australian *John/Jane Someones'* personal information to the system operator at the point of care during a search as well as the general public. The latter depends on local physical security measures such as ensuring system and/or computer monitor is not read by other individuals. From July 2012 a search may list 1,000s of *John/Jane Someones* personal details if their name is not unique and is a major risk to patient privacy.

[14] Security and Access Framework http://www.nehta.gov.au/component/docman/doc_download/877-security-and-access-framework

Recommendation 7: *That the legislation address the possibility of unauthorised access to PCEHR information though inappropriate search algorithms.*

Q2. Should portals for consumer registration be provided by organisations other than health related organisations, including government organisations?

Recommendation 8: *That the Legislation not limit the use of non-health organisations as registration authorities provided they are certified by an independent authorised certification body / organisation.*

Recommendation 9: *That the PCEHR legislation include the roles and responsibilities of both bodies (registration and certification organisations) and other criteria that these bodies would need to comply with (including compliance with the Privacy Act and requirement to be bound by Australian law).*

The College believes that the requirement to provide physical identification artefacts such as such as passports or birth certificates for review by portal service providers are not practical for Australians living in remote communities. The legislation should enable electronic enrolment services based on identification artefacts which can be verified electronically, eg Medicare number (which is accurate enough to produce IHI numbers), Tax File Number, bank account details, etc.

Recommendation 10: *That the PCEHR legislation include the option of non-physical identification artefacts for enrolment.*

Proposal 3: Legislation would provide a broad framework permitting an individual to participate in the PCEHR system through an authorised representative.

The College supports this approach.

Proposal 4: Administrative and/or policy arrangements would provide the detail for how a person can be recognised by the PCEHR system as an authorised representative.

The College supports this approach.

Proposal 5: Legislation would not prescribe eligibility criteria for authorised representatives, but would recognise authorised representatives established under existing Commonwealth, state and territory laws.

The College supports this approach.

Q3. What possible barriers are there to the participation of individuals through their authorised representatives?

Recommendation 11: *That the Department consider when drafting legislation that some patients change their minds frequently and may wish to change authorised representatives once or*

more per year. The PCEHR system operator will need to audit the changes to mitigate risks that might be associated with often-changed authorised representatives.

Proposal 6: Legislation will not prescribe the age at which a person under 18 years of age is presumed to have capacity to manage their own PCEHR.

The College supports this approach.

Proposal 7: Consistent with the approach taken by Medicare Australia, an administrative/policy framework will provide for participation in the PCEHR system by minors. The general participation arrangements will apply as follows:

- up to 14 years of age – a parent or legal guardian will be responsible for the child's PCEHR, including whether to register the child for a PCEHR and managing the access controls of the child's PCEHR;
- 14 to 18 years of age – a young person will be presumed to have capacity to make decisions in respect of their PCEHR. If the child elects to manage their own PCEHR they can decide whether or not to participate in the PCEHR system and manage the access controls of their PCEHR including choosing whether to allow their parent or legal guardian access. If a young person chooses not to manage their own PCEHR, the parent or legal guardian would continue to manage the young person's PCEHR;
- 18 years and over – an individual takes responsibility for their own PCEHR. The PCEHR system will no longer allow a parent or legal guardian to access the individual's PCEHR unless the individual grants access to the parent or guardian as a nominated representative. Alternatively, if the individual has limited or no capacity, the arrangements for authorised representatives will apply and the representative will need to provide evidence of their legal authority for verification by the PCEHR system operator.

Requests by minors under 14 years of age to manage their own PCEHR will be considered on a case by case basis by the PCEHR system operator.

The College supports this approach.

Q4. What other circumstances might need to be accommodated in the administrative arrangements for minors?

Recommendation 12: *That the Department consider cases where a minor is responsible for their own PCEHR in the same way as those 18 years and over.*

It is logical to assume such minors seek confidentiality and control of information about themselves in the first instance. No-one but the individual concerned and their authorised or nominated representatives and those with legal authority have the right to inform the parents or any other third party of PCEHR contents.

Proposal 8: The PCEHR system will support the creation and use of a PCEHR using a pseudonymous identity and healthcare identifier.

The College supports this approach in principle, provided that linkage to the user's true identity can be properly protected (for instance in cases where the patient's safety may be at risk if this was disclosed or identified by a third party).

Q5. What are the possible risks related to the creation and use of a pseudonymous PCEHR?

In an emergency, clinician access would be desirable, however this would be precluded if the pseudonymous records are not linked to an individual's PCEHR - if the PCEHR is intended for patient use then this is not an issue, however if it is expected that doctors will use the PCEHR to make clinical decisions with respect to patient care then this is an issue that would need to be properly addressed.

Proposal 9: Legislation would specify that in order to be eligible to register for the PCEHR system a healthcare provider organisation must:

- have a HPI-O;
- conform to specified technological requirements; and
- agree to prescribed terms and conditions.

The College supports this approach.

Proposal 10: Legislation would provide a framework for standards with which healthcare provider organisations must comply.

The College supports this approach.

Proposal 11: Legislation would provide authority for the making of terms and conditions which will apply to a healthcare provider organisation regarding the authorisation and identification of eligible users of the PCEHR system within the organisation.

The legislation will describe that, to be eligible as an authorised user:

- healthcare providers must have an HPI-I and be identifiable in the healthcare provider organisation's local system; and
- other individuals within a healthcare provider organisation, such as contracted service providers and administrative staff, must be identifiable in the healthcare provider organisation's local system and have a legitimate need to access the PCEHR system.

The College supports this approach.

Q6. Are there other terms and conditions that should apply to healthcare provider organisations in regulating the eligibility of authorised users?

Any additional terms and conditions to be applied to authorised users should be made clear in the legislation along with the implications of breech of these terms.

Proposal 12: Legislation would provide a framework for rules and standards with which a nominated healthcare provider must comply in authoring and managing a shared health summary.

The College supports this approach.

Proposal 13: The legislation may set out a framework for the rules and standards that relate to the authorship of other PCEHR documents.

The College supports this approach in principle but would seek to provide further comment if any proposed rules and standards that are intended to be applied to specific PCEHR documents have been drafted and made public.

Q7. What are the essential rules and standards with which a nominated healthcare provider should comply in relation to authoring and managing a shared health summary?

The College does not have an official position on this subject this time, however the College supports the comments expressed by the Office of the Australian Information Commissioner (as per its submission related to the draft PCEHR ConOps document[15]) and would also recommend that DOHA review the information governance requirements, standards and legal requirements that are applicable to the NHS EHR as published on the UK NHS Connecting for Health Website[16].

Proposal 14: The legislation would establish the PCEHR system operator, prescribe the operator's functions and responsibilities and establish an administrative framework for setting the service levels and operational rules that the PCEHR system operator would need to meet.

The College supports this approach.

Proposal 15: The HI Act would be amended to explicitly support the use of healthcare identifiers by the PCEHR system operator.

The College supports this approach, provided that the scope and restrictions of use of healthcare identifiers on the PCEHR system operator is clearly defined and that the PCEHR system operator be also subject to the penalty schema under the HI Act where there is proven negligence or breech of its responsibilities under the Act.

Q8. What are the essential obligations that should apply to the PCEHR system operator?

Recommendation 13: *That the following obligations to be required of the PCEHR system operator:*

1. The PCEHR operator should be:

a. a Legal Entity in Australia;

[15] http://www.oaic.gov.au/publications/submissions/2011-06%20Submission%20on%20PCEHR%20ConOps%20FINAL.html

[16] http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igfaqs

b. an entity that is fully independent of Government, PCEHR performance assessment and audit bodies. The PCEHR operator may be a private sector business, a NGO or statutory body); and

c. subject to privacy obligations under Australian law (including the Privacy Act)

2. Service Levels / Performance requirements should be broadly covered in the PCEHR legislation (as high level objectives and targets), however detailed performance and service level requirements (including detailed metrics/ measures to be used, how they will be assessed and penalties for not meeting targets etc) should be included as part of the contract and service level agreement with the PCEHR operator - the performance and service level information should be published and made available to the public online (via website)

3. Directors of the System Operator must be subject to Australian law.

Proposal 16: The legislation would define repository operators to include registry operators and provide a framework for the regulation of PCEHR-conformant repositories, including:

• a framework for allocating identifiers to PCEHR-conformant repositories;

• requiring that all health information used for PCEHR system purposes must be held in Australia; and

• requiring that repository operators are a legal entity within Australia.

The College supports this approach with:

Recommendation 14: *That the PCEHR legislation include the requirement that repository operators be subject to privacy obligations under Australian law (including the Privacy Act).*

Proposal 17: The legislation would establish the role of the National Repositories Service, identify its operator and provide any unique criteria which will apply to the National Repositories Service.

The College supports this approach.

Proposal 18: Relevant legislation would be amended to enable specific data sources held by Medicare Australia to be compliant repositories for the PCEHR system.

The College supports this approach.

Q9. What are the essential obligations that should be met by repository operators?

The College supports this approach with:

Recommendation 15: *That the roles and responsibilities of Repository operators be specified in the PCEHR legislation.*

Recommendation 16: *That the repository operators be subject to Australian law (including the Privacy Act).*

Recommendation 17: *That the repository operators require certification in accordance with certification criteria specified in the PCEHR legislation.*

Q10. What additional criteria might be applicable to the national repositories?

Any additional criteria or requirements to be applied to the national repositories should be made clear in the legislation along with the implications of breech of these requirements.

Proposal 19: The legislation will authorise the use of data held by Medicare Australia, DVA and the Department of Defence as trusted data sources for identity verification purposes.

The College supports this approach.

Proposal 20: The legislation will allow for future trusted data sources to be identified through regulations.

The College does not support this approach. This is important since amendment of regulations would allow social security, passport / immigration, tax and financial information data sources to be very easily included at a future time.

Recommendation 18: *That future addition of trusted data sources require formal amendment of the PCEHR legislation.*

Q11. Are there any other trusted data sources that should be included in the legislation from the outset of the PCEHR system?

Recommendation 19: *That no other "trusted" data sources be considered at this stage. Any future additions of "trusted" data sources needs to be made by amendment of the PCEHR legislation and not through regulations (this is important since amendment of regulations would allow social security, passport / immigration, tax and financial information data sources to be very easily included at a future time).*

Recommendation 20: *That the legislation provide both a definition of and purpose of using a "trusted data source" and specify how it will be used by the PCEHR system and its operator(s).*

Proposal 21: The legislation will provide for the participation of portal providers.

The College supports this approach with:

Recommendation 21: *That the roles and responsibilities of portal providers be specified in the PCEHR legislation.*

Recommendation 22: *That the portal providers be subject to Australian law (including the Privacy Act).*

Recommendation 23: *That the portal providers require certification in accordance with certification criteria specified in the PCEHR legislation.*

Proposal 22: The legislation will provide a framework for the regulation of PCEHR-conformant portals, including:

• a framework for allocating identifiers to PCEHR-conformant portals;

• requiring that all servers used for PCEHR system purposes and all demographic information used for PCEHR system purposes must be held in Australia; and

• requiring that portal providers are a legal entity within Australia.

The College supports this approach.

Q12. Are there any other essential requirements for portal providers?

Recommendation 24: *That all demographic or other personal information captured or used for PCEHR system purposes must be held in Australia.*

Proposal 23: The assignment of intellectual property rights for the PCEHR system would be based in either legislation or contract. The changes required will be further developed as feedback is received as part of the consultation process.

The College supports this approach.

Q13. Are you aware of specific examples of information for which intellectual property rights might present a significant barrier to the use of the information in the PCEHR system?

Translational biomedicine often refers to interventions founded on basic or clinical research. One clinician's intellectual property rights may present a significant barrier to the use of translational data by other clinical and biomedical researchers (One clinician may enter data into the PCEHR system and another clinician or researcher may draw on the data for translational research). This is particularly so in the context of data mining and related research methods as well as other research approaches.

Examples provided during consultation in Canberra referred to Specialists but anecdotal evidence suggests GPs are more likely to have IP concerns[17]

Proposal 24: The legislation would require retention of documents which have been indexed/accessed by the PCEHR system for 15 years since last action on record (or in the case of a minor, until they are 30 years of age).

The College supports this approach in principle. Please refer to the **ACHI response to Q14 below**.

[17] Hamblin, J. Breen v Williams - Right of Access to Medical Records Denied http://www.austlii.edu.au/au/journals/PLPR/1994/109.html

Q14. Can you identify any other options for records retention and can you identify any other issues regarding records management that have not been considered in this paper?

Retention should also consider permanent archival or data migration to a different system if the PCEHR system is decommissioned in the future or if the individual wishes to cease using their PCEHR (i.e. opt-out) and transfer their health information to a different system of their choice

This is a complex issue as current national (in particular the National Archives Act) and state legislation (and health regulations) specify different requirements with regard to retention of records. In addition, there is a need to recognise the rights of the individual to have the information retained (archived) or migrated to another system (in the event of a decommissioning of the PCEHR system) protected under specific PCEHR legislation (that should take precedence over state or other national archive legislation).

At what point do the State/Territory document retention laws apply? It should also be noted that there are different laws and regulations for medial and non-medical data.

Recommendation 25: *That the Department consider the legislative issues raised by permanent archival or data migration to a different system if the PCEHR system is decommissioned in the future or if the individual wishes to cease using their PCEHR.*

Proposal 25: Legislation would set out the individual's role in setting access controls, authorising others to access their PCEHR, choosing which information is published to and accessible through their PCEHR, viewing an activity history for their PCEHR and making enquiries and complaints.

The College supports this approach.

Q15. Are there additional access functions for individuals that need to be included in legislation?

Given that this is a patient controlled record (and assuming it is primarily for patient use), it is reasonable for a patient to be given the right to request to have their record deleted (and not just deactivated) if they wish to "opt-out". In addition, at any time over the period they are registered on the PCEHR system and have a PCEHR record (including pseudonymous record(s)) - whether active or not, the individual should have the right to have their information transferred to another system (or transferred to media – e.g. DVD ROM / blue ray disc, USB memory / storage device) - this right should include the ability / option to transfer their record information to another system or media if they decide to 'opt-out' and have their PCEHR information deleted from the PCEHR system.

Recommendation 26: *That the Department consider the legislative issues raised by patients requesting to have their record deleted or transferred to another.*

Proposal 26: The broad framework which permits an individual to participate in the PCEHR system through an authorised representative (see proposal 3) will provide the necessary legislative support for access by authorised representatives.

The College supports this approach in principle.

Q16. Should any specific restrictions apply to the extent to which an authorised representative can act on behalf of the individual within the PCEHR system?

The 'mandate' (e.g. power of attorney) provided explicitly to 'authorised representatives' to act on behalf of an individual should be properly obtained and verified as being legitimate under Australian law and hence all rights of the individual would be transferred to the authorised representative with regard to the PCEHR - including decisions relating to 'opt-in' or 'opt-out', creation, deactivation, deletion or archival of the individual's PCEHR and any pseudonymous PCEHR's.

To ensure that only representatives that are duly authorised access the PCEHR, the auditing capability of the PCEHR system needs to include 'authorised representatives'. The cost and resource implications of such audit trails is currently unclear[18].

Recommendation 27: *That the legislation require that a comprehensive audit trail of all PCEHR activity / transactions related to changes made, information provided / uploaded, information accessed / downloaded or changes made relating to access control settings, or any other update of the record made by individuals, authorised or nominated representatives should be kept and be easily retrievable for review.*

Proposal 27: The legislation would allow an individual to nominate one or more persons to be their nominated representative for the purpose of viewing the individual's PCEHR.

The College supports this approach.

Q17. Are there any other essential or additional requirements or obligations of a nominated representative that should be supported in the PCEHR legislative framework?

Any specific requirements or obligations to be applied to a nominated representative should be made clear in the legislation along with the implications of breech of these requirements.

Proposal 28: Legislation would not prescribe eligibility criteria for nominated representatives, thereby allowing for representation by minors.

The College supports this approach.

Q18. Are there any reasons why an individual should not be able to choose a minor as their nominated representative?

With regard to an individual's right to nominate a minor as their representative, it would be prudent to have alignment and consistency with Medicare requirements, with legislation of a minimum age of 14 for a minor being a reasonable age.

Recommendation 28: *That the ability to choose a minor as the nominated representative be aligned and consistent with Medicare requirements regulations and specified in the PCEHR legislation.*

[18] SA Health Response to the ConOps, last bullet point
www.yourhealth.gov.au/internet/yourhealth/blog.nsf/2324504E774C2558CA2578DF00155D61/$FILE/SA%20Health.pdf

Q19. Would it be desirable to include any other eligibility criteria for a nominated representative?

The eligibility criteria to be applied to a nominated representative should be specified in the PCEHR legislation.

Proposal 29: Legislation is required to define authorised users who may access a PCEHR when they have been granted permission to do so by the healthcare provider organisation they work for and in line with the access control settings established by the individual.

The College supports this approach.

Q20. Are there additional issues in relation to authorised users that should be addressed in the legislation or regulations?

The College believes that feedback from the Australian Health Informatics Education Council[19] with regard to professional education needs to be reflected in the Legislative Issues Paper. Our current workforce shortage of e-health professionals is a substantial *"roadblock"* to enabling the PCEHR system [20] [21]. Professional, undergraduate and postgraduate clinical students and their teachers must be able to access records stored on the system as a learning tool. For example, undergraduate medical students spend extensive periods of time over several years on clinical placement and will inevitably require access to the PCEHR system during that time. Access to the system at pertinent stages of university training will facilitate the development of formal and robust biomedical and health informatics education modules in curricula. Our graduates need some experience of the PCEHR system before using it in a "live" practice environment. There is no consideration of such in the Paper.

Recommendation 29: *That the Department consider training environments for operation and management of the PCEHR.*

Proposal 30: Emergency PCEHR access is already provided under existing privacy and health legislation.

Recommendation 30: *That the PCEHR operator (and its sub-contractors) and all providers (including health and ICT providers, portal and repository operators) and organisations / agencies / entities that use, maintain, operate or provide data or services to the PCEHR system (as part of its normal operations, support maintenance or enhancement) should be subject to the Privacy Act and privacy obligations under Australian law.*

[19] See www.AHIEC.org.au

[20] www.yourhealth.gov.au/internet/yourhealth/.../HIMAA%20submission.pdf

[21] www.achi.org.au/docs/ACHI_Response-PCEHR_ConOps_V1.2.pdf

Q21. Should there be additional legislative provisions for emergency access to PCEHR information?

The College does not see the need for additional legislative provisions to address emergency access to personal health information that are not already addressed in existing privacy and health legislation.

Proposal 31: In relation to the system operator and portal operators, the legislation should ensure that a body may not perform that role unless it is subject to the Privacy Act.

The College supports this approach.

Proposal 32: In relation to repository operators, the legislation should ensure that a body may not perform that role unless it is subject to privacy obligations under Australian law.

The College supports this approach.

Q22. Will this provide the necessary level of protection for personal information uploaded to the PCEHR system?

Recommendation 31: *That personal information uploaded by individuals or PCEHR authorised health providers should be subject to the Privacy Act and privacy obligations under Australian law.*

Q23. What privacy legislation should apply to repository operators?

As per the **College response to Q9 above**, repository operators should be subject to Australian law including the Privacy Act.

Proposal 33: Healthcare providers will be subject to the privacy coverage provided by existing law.

The College supports this approach.

Q24. Are there any reasons why clinical information downloaded from the PCEHR system should be required to be handled differently to other information held by a healthcare provider in their local records?

Q25. If so, how could the practical difficulties be overcome?

The requirement to comply with Australian law (including all relevant Commonwealth and State Privacy, Health and other relevant legislation and regulations) with regard to the handling of personal health information (which includes clinical information) should apply equally to PCEHR clinical information that is downloaded or uploaded, accessed, stored, modified, amended, deleted transferred or exchanged with other systems.

Proposal 34: The legislation would not displace the exceptions to the prohibition on use and disclosure of health information in the Privacy Act. The Commonwealth will work with states and

territories to identify any existing reporting or secrecy provisions that may impact on the operation of the PCEHR system.

The College supports this approach in principle.

Recommendation 32: *That the PCEHR legislation specifically refer to existing exceptions and additional provisions to protect the secondary uses and disclosure of personal information permitted under the Privacy Act.*

Recommendation 33: *That the PCEHR legislation specifically address the secondary use of pseudonymous personal health information for the purposes of epidemiology, population health and research purposes. This should include:*

a. the criteria, constraints and limitations for authorised secondary use

b. the requirement for consent from the individual to 'opt-in' to allow access to this information,

c. the mechanism of pseudonymisation of personal health information to be employed

d. the legal requirements and obligations of authorised secondary users of PCEHR personal health information

e. the requirements and process of registration of authorised secondary users of PCEHR personal health information, and

f. the penalties that would apply for inappropriate use or disclosure of this information

Q26. Are you able to provide examples of existing reporting or secrecy provisions that might impact on the PCEHR system operations?

The College is considering this issue and may offer comment at a later stage.

Proposal 35: The legislation will provide a framework to support ongoing security of the PCEHR system, but will not set technical requirements, to allow for quick and flexible responses to technological change.

The College supports this approach in principle.

Q27. Are there technical aspects of the PCEHR system design that are so critical to security and sufficiently stable over time as to warrant inclusion in the legislation or regulations?

Recommendation 34: *That the PCEHR systems be required to implement robust data encryption technologies to electronically protect all Personal Information (PI) that is stored or electronically transmitted or exchanged with other authorised systems. The data encryption technology used to encrypt PI stored in the PCEHR system and all its datastores and repositories should be compliant with the Advanced Encryption Standard (AES) as certified by the National Institute of Standards Technology (NIST) or an equivalent or more secure data encryption standard as certified by NIST.*

Recommendation 35: *That all agencies (including Commonwealth, State government or NGOs), private sector organisations and individuals (i.e. not just healthcare providers and organisations) that are permitted access to PCEHR systems or PCEHR information stored in repositories or*

datastores (e.g. for the purpose of system administration, operation, research or any other authorised purpose) should at a minimum comply with privacy, security and confidentiality requirements as specified in existing commonwealth and state privacy and health record legislation.

Recommendation 36: *That specific PCEHR legislation should include specification of the purposes for which authorised access to the PCEHR systems and data will be granted, administered, monitored and how privacy and security breaches will be dealt with (i.e. enforcement, penalties etc.)*

Proposal 36: Criminal offences would be included in PCEHR legislation covering officeholders or other legal entities involved in the management or control of the healthcare provider, to address:

- failure of a registered healthcare provider to notify the PCEHR system operator within a specified period when it ceases to meet the requirements for registration to participate in the PCEHR system;
- requests for and receipt of a record from the PCEHR system by a healthcare provider, when the provider or her/his requesting employer or contractor is not authorised to do so; and failure of a registered healthcare provider to meet audit trail or other record-keeping obligations imposed by the legislation.

The College supports this approach.

Q28. Is the size of the penalty (50 penalty units or $5,500) used in the HI Service appropriate for the PCEHR system?

The College believes that this level of penalty is appropriate for unauthorised PCEHR access by individuals.

The College believes that this level of penalty is inappropriate for unauthorised PCEHR access by organisations or individuals acting for organisations.

Recommendation 37: *That the Department consider more severe penalties (including imprisonment) for unauthorised PCEHR access by organisations or individuals acting for organisations.*

Q29. Is it appropriate to impose a penalty on the individual who requests a record from the PCEHR system when not entitled to do so?

The College believes that intentional requests for unauthorised PCEHR access should be penalised.

Proposal 37: Criminal offences would be included in PCEHR legislation which relates to the participation in the PCEHR system by a repository or portal operator, where that body has failed to meet or maintain the requirements for participation in the system.

The College supports this approach.

Q30. What specific breaches of requirements should result in an offence and penalty for repository or portal operators?

The College believes that any negligent and/or intentional acts that result in personal information being able to be accessed without authorisation should be penalised.

Recommendation 38: *That the legislation include provisions for penalties (including imprisonment) for any negligent and/or intentional acts by repository or portal operators that result in PCEHR privacy breaches.*

Proposal 38: The legislation may not include an obligation of confidentiality on the PCEHR system operator or its employees or contractors. Instead, inappropriate handling of personal information would be dealt with under existing privacy, disciplinary or criminal law.

The College believes that the PCEHR legislation needs to be clear and unambiguous regarding the confidentiality obligations of all parties involved in the PCEHR. The Department may consider publishing a "PCEHR Privacy Guide" for the abundance of clarity.

Recommendation 39: *That the PCEHR legislation be abundantly clear and unambiguous regarding confidentiality obligations of all parties involved in the PCEHR.*

Q31. If the system operator is an agency and its employees are subject to the Code, would these disciplinary measures be sufficient?

The College is not clear what constitutes "the Code" – please explain.

Q32. If the PCEHR system operator is a private sector organisation would additional mechanisms be required?

A gap analysis to establish any difference in disciplinary measures between government agencies and private operators would be useful to ensure there are no inconsistencies regarding obligations and penalties.

Recommendation 40: *That the Department ensure a gap analysis is undertaken regarding any differences in PCEHR disciplinary measures between government agencies and private operators.*

Proposal 39: The Commonwealth will assess the coverage of existing Commonwealth offences to determine whether specific PCEHR offences are needed to better enable the Commonwealth to have jurisdiction in PCEHR-related identity crime matters.

The College supports this approach.

Proposal 40: The Commonwealth will seek to amend its existing computer offence provisions to remove existing constitutional limitations. This will enable the offences to apply to all PCEHR-related cyber crime matters.

The College supports this approach.

Q33. What are your views about the preferred governance structures for the PCEHR system and national e-health elements more broadly?

Recommendation 41: *That the Governance framework be referred to in the PCEHR legislation and:*

a. provide a high level of transparency and accountability

b. include engagement of the critically necessary stakeholder communities

c. provide a comprehensive list of all governance bodies and entities, inter-relationships between the entities, lines of reporting and authority, detailed roles and responsibilities, process for constituting and establishing governance entities, list of constituents of the governance entities, schedule of meetings of governance entities

d. reports, meeting agendas, minutes and other documentation to be made accessible to the public online (via a publicly accessible website) for review

e. mechanism for registering governance related issues or complaints online via a publicly accessible website that will be addressed by the appropriate governance entity (with communication of the issue status, any actions taken and final outcome from the appropriate governance entity to the person or organisation registering the issue)

f. detail any legal requirements of the various governance bodies or entities described under the PCEHR Governance arrangements that may be specified in the proposed PCEHR legislation, in particular with regard to the roles and responsibilities of relevant agencies and organisations authorised to perform or assist with the following:

i. design, develop, implement, maintain, support, operate, monitor, audit or assess the performance of the PCEHR system (including access to the system and PCEHR information);

ii. investigate alleged criminal activity or breach associated with operation, access to, or management of the PCEHR system; or

iii. investigate complaints from individuals (or authorised or nominated persons) or health providers relating to PCEHR access (and controls), record creation, population of the records, record content or unauthorised use or misuse of PCEHR information.

Proposal 41: The Commonwealth, in collaboration with the states and territories, will develop proposals for a single entry point for PCEHR privacy complaints which are then referred to the appropriate regulator(s).

The College supports this approach.

Q34. What would be your preferred single entry point for PCEHR privacy complaints?

The College believes that a single and government-independent body that has neither commercial nor political interests would be the preferred entry-point for PCEHR complaints. Such a body, similar to an Ombudsman, should be government-funded and report directly to the Health Minister. The remit of this body may not be limited to privacy, but could handle all relevant PCEHR complaints.

Recommendation 42: *That an Ombudsman-like body be set up to handle PCEHR complaints.*

Contributors

Lead Authors: Paul Clarke, Juanita Fernando, Klaus Veil

Additional Contributors: ...

Review and other contributions: Fellows and Members of ACHI