Australian Government

Office of the Australian Information Commissioner

Inquiry into the provisions of the Personally Controlled Electronic Health Records Bill 2011 and a related bill

Submission to the Senate Standing Committee on Community Affairs

January 2012

Submission by Timothy Pilgrim, Australian Privacy Commissioner

Contents

Recommendations 1
The Office of the Australian Information Commissioner 3
Involvement of the OAIC in the PCEHR System 4
Comments on the Inquiry 6
Background 6
Interaction with the Privacy Act 7
Information Commissioner's Roles and Powers 8
The Independent Advisory Council 11
Complaints Handling 12
Data Security 13
Civil Penalties and other Remedies 14
PCEHR Rules 16
Definitions 16
Reporting and Review of the PCEHR Bill 17
PCEHR (Consequential Amendments) Bill 17

Recommendations

The OAIC notes that the Personally Controlled Electronic Health Records Bill 2011 (PCEHR Bill)[1] and a related bill[2] lay the foundations for the Australian Government's PCEHR System which aims to improve the quality, safety and access to health and medical care for consumers.

The OAIC strongly supports introducing enabling legislation to accompany the PCEHR System. Ensuring that this legislation appropriately protects individuals' personal information is fundamental to establishing and maintaining public confidence in the system.

The OAIC makes the following recommendations aimed at enhancing the provisions of the Bill to achieve that objective:

1. The interaction between the PCEHR Bill and the Privacy Act could be made more certain by:

   i. amending the Privacy Act to confirm that the Information Commissioner may investigate anyone who may have contravened a civil penalty provision in the PCEHR Bill (even if that person would otherwise be exempt under the Privacy Act);

   ii. explaining when a contravention of the PCEHR Bill would be an interference with privacy under s 13 of the Privacy Act, and when it would be an interference with privacy under s 13A; and

   iii. consistent with the wording in ss 13 and 13A of the Privacy Act, referring to 'an interference with the privacy of an individual' in s 73(a) of the PCEHR Bill, rather than 'an interference with the privacy of a consumer'.

2. The PCEHR Bill should ensure that the Information Commissioner can invoke all the investigative powers provided under Part V of the Privacy Act, including own motion investigations.

3. The PCEHR Bill should clarify the Information Commissioner's powers and specifically provide which of the Privacy Act mechanisms may be utilised following a possible contravention of the PCEHR Bill.

4. The PCEHR Bill should specify that the System Operator will be subject to the Privacy Act and consequential amendments made to the Privacy Act to also ensure this.

5. The Independent Advisory Council should include at least one member with experience or knowledge of privacy.

6. The PCEHR Bill (or at a minimum, the PCEHR Rules) should clarify the complaints

---

[1] See: http://www.comlaw.gov.au/Details/C2011B00258

[2] The OAIC notes that the 'related bill' refers to the Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 (Consequentials Bill).

handling process for privacy complaints.

7. The PCEHR Bill should include data security provisions which would apply uniformly to the System Operator, portal operators and repository operators.

8. The PCEHR Bill should clarify the Information Commissioner's power to investigate a possible contravention of the civil penalty provisions, where the contravention is not in connection with a consumer's health information.

9. The data breach notification requirements which currently only apply to the System Operator, registered repository operators and registered portal operators, should be extended to other entities which may access consumers' health information from the PCEHR system.

10. The civil penalty provisions in Part 4 of the PCEHR Bill should apply to health information that was originally obtained from the PCEHR system.

11. The Senate Committee should seek clarification of whether 'identifying information' and 'healthcare identifiers' handled under the new Division 2A, Part 3 of the Healthcare Identifiers Act 2010 (Cth) (HI Act), would be covered by the civil penalty provisions in Division 1, Part 4 of the PCEHR Bill.

12. Consideration should be given to ensuring there are appropriate remedies available where an entity, such as a healthcare provider organisation, breaches a PCEHR Rule.

13. The Senate Committee should seek clarification of the reasons for using the terms 'collecting' health information and 'obtaining' health information and any implications of using these different terms.

14. All privacy regulators should be required to compile and report their statistics about complaints received and investigations undertaken in relation to PCEHRs or the PCEHR system.

15. The review under s 108 of the PCEHR Bill should also include an assessment of the adequacy of privacy protections under the PCEHR legislation.

16. The Consequentials Bill should specify the particular purpose for which repository operators, portal operators and the System Operator may collect, use or disclose healthcare identifiers and, for the System Operator, identifying information.

The Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (the OAIC) is established by the *Australian Information Commissioner Act 2010* (Cth)[3] (the AIC Act) and commenced operation on 1 November 2010. The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner. The former Office of the Privacy Commissioner was integrated into the OAIC on 1 November 2010.

The OAIC brings together the functions of information policy, and independent oversight of privacy protection and freedom of information (FOI), in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act – providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)[4], and
- the privacy functions, set out in s 9 of the AIC Act – protecting the privacy of individuals in accordance with the *Privacy Act 1988* (Cth)[5] (the Privacy Act) and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

As the national privacy regulator the OAIC can provide general advice on privacy issues and the application of the Privacy Act.

The Privacy Act applies to 'personal information', which is defined in s 6(1) as information or an opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained from that information. The Privacy Act contains eleven Information Privacy Principles (IPPs) which apply to Australian and ACT Government agencies. It also includes ten National Privacy Principles (NPPs) which generally apply to private sector

[3] www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP201046680

[4] www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401430

[5] www.comlaw.gov.au/comlaw%5Cmanagement.nsf/lookupindexpagesbyid/IP200401860

organisations, but which do not apply to certain exempt organisations including some small businesses and State or Territory authorities.[6]

Health information is a subset of personal information and also defined in s 6(1) of the Privacy Act. In the PCEHR Bill, the information included in a consumer's PCEHR is referred to as health information. The definition of health information in the PCEHR Bill and the Privacy Act is substantially the same. The only difference is that under the PCEHR Bill the definition uses the term healthcare rather than health service. Despite this difference, it is intended that health information have same meaning under the PCEHR Bill as it does under the Privacy Act.[7]

Involvement of the OAIC in the PCEHR System

The OAIC has been actively involved to ensure that privacy protections are built into the PCEHR System. The OAIC made submissions to Department of Health and Ageing (DoHA) on the *PCEHR System: Legislation Issues Paper*, in August 2011[8] and the *draft Concept of Operations relating to the introduction of a PCEHR system*, in June 2011.[9] More recently, the OAIC made a submission to DoHA on the *Exposure Draft PCEHR Bill 2011, Exposure Draft PCEHR (Consequential Amendments) Bill 2011* and *PCEHR System: Exposure Draft Legislation (Companion Document)* (Draft Bill), in October 2011.[10]

The OAIC acknowledges that many of the recommendations in its submission to DoHA on the Draft Bill were adopted in full or in part. Some of the recommendations which were adopted include:

- The PCEHR Bill now includes that one of the functions of the System Operator is to 'educate consumers, participants in the PCEHR system and members of the public about the PCEHR system'.

- Section 63 of the PCEHR Bill now provides that a participant is authorised to collect, use or disclose personal information in response to a request by the System Operator for the purpose of performing a function or exercising a power,[11] clearly describing the limited purpose for which the System Operator can collect health

[6] Information relating to the operation of the Privacy Act can be found on the OAIC website at: http://www.privacy.gov.au/law/act

[7] Explanatory Memorandum to the PCEHR Bill, p 5.

[8] See: http://www.oaic.gov.au/publications/submissions/2011_08_submission_personally_controlled_ehealth.html

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

[10] See: http://www.oaic.gov.au/publications/submissions/2011_10_PCEHR_submission.html

[11] Section 63(b), PCEHR Bill.

information.

- Section 77 of the PCEHR Bill, through a new civil penalty provision, restricts contracted service providers (CSPs) (and others) from taking or holding records outside Australia.

- Section 48(d) of the PCEHR Bill requires that portal operators (as well as repository operators) that are State or Territory authorities, or an instrumentality of a State or Territory, be bound by either the Privacy Act or an equivalent State or Territory privacy law. The OAIC reiterates that this provision should apply to all portal and repository operators.

- The Explanatory Memorandum indicates that the System Operator may have regard to expert advice which is appropriate, including advice of the OAIC.[12]

- The Explanatory Memorandum indicates that the purpose of the data breach notification provisions (in Part 5, PCEHR Bill) is to allow the System Operator and the Information Commissioner to 'investigate, take corrective actions and help mitigate any loss or damage that may result from the breach'.[13]

The OAIC also notes that additional wording has been included in s 73 of the PCEHR Bill to the effect that an act or practice which would contravene the PCEHR Bill, but for a requirement relating to the state of mind of a person, is taken to be an interference with privacy covered by the Privacy Act. The OAIC supports this change, which makes certain that the Privacy Act still applies even when the contravention of the PCEHR Bill was by mistake.

The OAIC considers that these changes enhance the privacy protections provided by the PCEHR Bill. The changes create a more consistent and comprehensive regulatory framework for participants, in circumstances where different privacy laws and arrangements would otherwise apply.

However, some of the recommendations made in the OAIC's submission on the Draft Bill were not incorporated in the PCEHR Bill. These recommendations are the basis for the detailed comments below and emphasise the provisions which the OAIC believes could benefit from further clarity, in particular, with respect to the privacy protections, the interaction between the Bill and the Privacy Act and the Information Commissioner's new functions and powers.

[12] Explanatory Memorandum to the PCEHR Bill, p 13.

[13] Explanatory Memorandum to the PCEHR Bill, p 48.

Comments on the Inquiry

Background

The OAIC welcomes the opportunity to make a submission to the Senate Community Affairs Legislation Committee (Senate Committee) regarding its inquiry into provisions of the PCEHR Bill 2011, Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 (Consequentials Bill) and Explanatory Memoranda.[14] The OAIC notes that both the PCEHR Bill and Consequentials Bill are accompanied by an Explanatory Memorandum, however, all references in this submission to 'Explanatory Memorandum' mean the Explanatory Memorandum to the PCEHR Bill.

In May 2010, the Australian Government announced $466.7 million to fund the creation of the PCEHR System over two years. The OAIC understands the System is being developed as part of the national e-health program to drive improvements in quality, safety and access to health and medical care. It is intended that individuals will be able to register for a PCEHR online from July 2012.

Ensuring that privacy is adequately addressed is fundamental to achieving community trust in the PCEHR System, and gaining consumer acceptance and take-up of the System. This is particularly important given the sensitive nature of the information being held in the PCEHRs. Over the course of a lifetime, a significant proportion of people may experience conditions which they view as highly sensitive and for which they need extra assurance that related information will be handled privately. For example, it is estimated that around 20% of Australians will experience mental illness during their lives and most will experience a mental health problem.[15]

On 23 November 2011, the PCEHR Bill and the Consequentials Bill were both tabled in Parliament. On 25 November 2011 the Senate referred the Bills for inquiry and report. The OAIC makes a number of recommendations to the Senate Committee which would clarify and enhance the privacy protections applying to information collected and handled under PCEHR legislation. These recommendations, which are detailed below, build on the recommendations and comments made in the OAIC's submission to DoHA in relation to the exposure draft of the Bill.

---

[14] See: http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;adv=yes;orderBy=priority,title;page=0;query=Dataset_Phrase%3A%22billhome%22%20ParliamentNumber%3A%2243%22%20Portfolio_Phrase%3A%22health%20and%20ageing%22;rec=13;resCount=Default

[15] *A Healthier Future For All Australians*, Interim Report December 2008, p 239. See: http://www.health.gov.au/internet/nhhrc/publishing.nsf/Content/interim-report-december-2008

Interaction with the Privacy Act

The OAIC believes that the interaction between the PCEHR Bill and the Privacy Act remains uncertain in several aspects. Initially, greater clarity could be achieved by amending the Privacy Act to confirm that the Information Commissioner may investigate anyone who may have contravened a civil penalty provision in the PCEHR Bill (even if that person would otherwise be exempt under the Privacy Act).

Further, the PCEHR Bill could also describe when a contravention of the PCEHR Bill would be an interference with privacy under s 13 of the Privacy Act, and when it would be an interference with privacy under s 13A. Section 13 currently describes interferences with the privacy of an individual by agencies (among other entities). Section 13A describes interferences with the privacy of an individual by organisations. Conceivably, an entity that contravenes the PCEHR Bill may not be an 'agency' or an 'organisation' as defined in the Privacy Act.[16] For example, individuals operating in a personal capacity or State or Territory authorities may contravene the PCEHR Bill but, except for s 73, they would not be subject to the Privacy Act.[17] Where one of these entities contravenes the civil penalty provisions in Division 1 of Part 4 of the PCEHR Bill, it may not be clear that the act or practice interferes with privacy under s 13 or s 13A of the Privacy Act.

Another effect of s 73 is that some uses or disclosures that are permissible under an exception to the NPPs (or IPPs), would be 'interferences with privacy' for the purposes of ss 13 and 13A of the Privacy Act. For example, under NPP 2.1(d), a healthcare provider organisation covered by the Privacy Act could disclose health information for research purposes in certain circumstances.[18] However, for health information included in a consumer's PCEHR, such a disclosure may be an 'interference with privacy' for the purposes of the Privacy Act as it is not specifically authorised in Part 4, Division 2 of the PCEHR Bill. It may therefore be appropriate to add a note at the end of ss 13 and 13A, which refers to s 73 of the PCEHR Bill and briefly describes the circumstances where a breach of the PCEHR Bill

[16] See the definition of 'agency' in s 6(1) of the Privacy Act and the definition of 'organisation' in s 6C of the Privacy Act

[17] Section 8(1) of the Privacy Act generally limits the coverage of the Privacy Act to staff members engaging in conduct in the performance of their duties. See also, the definition of 'organisation' in s 6C of the Privacy Act, which generally does not apply to State or Territory authority or a prescribed instrumentality of a State or Territory

[18] Under NPP 2.1(d) in Schedule 3 of the Privacy Act, an organisation may use or disclose personal information about an individual for a purpose other than the primary purpose of collection where if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety: (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and (iii) in the case of disclosure--the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information.

would be an 'interference with the privacy of an individual' under that section. As a guide, the Senate Committee could refer to Note 1 to s 13 of the Privacy Act, which states 'a contravention of the Healthcare Identifiers Act 2010, or of regulations made under that Act, is an interference with the privacy of an individual and is covered by this section (see subsection 29(1) of that Act)' as a means of addressing this issue.

Sections 13 and 13A prescribe acts or practices that are an 'interference with the privacy of an individual', rather than an 'interference with the privacy of a consumer' (s 73(a) of the PCEHR Bill). Similarly, Part V of the Privacy Act refers to complaints made 'by an individual about an act or practice that may be an interference with the privacy of the individual'.[19] To ensure consistency between these provisions in the Privacy Act and the reference to these provisions in s 73(a) of the PCEHR Bill, the OAIC recommends that s 73(a) refer to 'an interference with the privacy of an individual', rather than 'an interference with the privacy of a consumer'.

Information Commissioner's Roles and Powers

The OAIC considers that the PCEHR Bill remains unclear in relation to some of the Information Commissioner's powers, in particular, the Information Commissioner's auditing and investigative powers.

The Explanatory Memorandum explains in broad terms the investigative powers of the Information Commissioner under the PCEHR Bill:

- The Privacy Act will generally apply to the PCEHR System in respect of health information in consumers' PCEHRs. Amongst other things, this will allow the Information Commissioner to investigate any interference with privacy.[20]
- The main area where the provisions of the PCEHR Bill will prevail over the Privacy Act are in relation to the collection, use and disclosure of health information in a consumer's PCEHR.[21]
- If a civil penalty provision is not established, because a fault element cannot be made out, any unauthorised collection, use or disclosure of information will still be subject to the mechanisms available under the Privacy Act.[22] For example, the Information Commissioner would still have the power to investigate where a collection, use or disclosure is not authorised under Division 2 of Part 4.[23]

[19] See for example, s 36(1) of the Privacy Act.

[20] Explanatory Memorandum to the PCEHR Bill, p 2.

[21] Explanatory Memorandum to the PCEHR Bill, p 2.

[22] Section 73 of the PCEHR Bill.

[23] Explanatory Memorandum to the PCEHR Bill, p 38, 47.

System Operator

The OAIC submits that it is not sufficiently clear whether any future System Operator prescribed by the PCEHR Regulations would be subject to the Privacy Act.[24] While the Explanatory Memorandum states that 'the System Operator will be subject to the Privacy Act'[25], there is no corresponding provision in the PCEHR Bill.

As the OAIC understands, DoHA's intent is that the System Operator will come under the jurisdiction of the Privacy Act. Further, that the OAIC will provide comprehensive privacy oversight that will enable the Information Commissioner to conduct audits of the System Operator. DoHA has advised the OAIC that it intends for this to be achieved by establishing the System Operator as an 'agency' for the purposes of the Privacy Act.

There are strong reasons for ensuring that the Information Commissioner can audit the information handling practices of the System Operator. Among other things, this would aid the detection of unauthorised information access or modification, and any other breach of information security. Accordingly, audits of the System Operator would allow the OAIC to more effectively identify existing or potential privacy risks in the PCEHR System and ensure compliance with the regulatory framework.

Currently, the Information Commissioner has powers under the Privacy Act to compulsorily audit Australian and ACT government agencies' compliance with the IPPs.[26] The Commissioner also currently has the power to audit private sector organisations covered by the Privacy Act **but** only at the organisation's request.[27]

The Information Commissioner's audit power in s 27(1)(h) of the Privacy Act, applies to audits of agencies which are subjects to the IPPs. The definition of 'agency' includes (among other things) a Department or a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment. For certainty, the OAIC recommends that a note should be included in s 14 of the PCEHR Bill specifying that the System Operator is subject to the Privacy Act. Additionally, the Privacy Act should be amended so that the definition of 'agency' also includes the System Operator under the PCEHR Bill.

The OAIC is concerned that if these recommendations are not adopted, the Information Commissioner may be limited in his ability to conduct audits of the information handling practices of the System Operator.

[24] Section 14 of the PCEHR Bill. See also the definition of 'agency' in s 6(1) of the Privacy Act and the definition of 'organisation' in s 6C of the Privacy Act.
[25] Explanatory Memorandum to the PCEHR Bill, p 35.
[26] Section 27(1)(h) of the Privacy Act.
[27] Section 27(3) of the Privacy Act.

Investigative Powers

Section 73 of the PCEHR Bill makes an act or practice that contravenes the Bill an interference with privacy under the Privacy Act. The OAIC interprets s 73 of the PCEHR Bill to mean that the category of acts and practices which constitute an interference with privacy under ss13 and 13A is broadened. Accordingly, the practical effect of this is that the Information Commissioner will be able to undertake investigations into possible interferences with privacy in respect of health information in consumers' PCEHRs even if the interference would not otherwise be covered by the Privacy Act. However, the Information Commissioner's investigative powers in relation to possible contraventions of the PCEHR Bill need clarification.

The Explanatory Memorandum states that the Information Commissioner will be able to investigate any interference with privacy in respect of health information in consumers' PCEHRs.[28] In the OAIC's opinion, this demonstrates an intention that the Information Commissioner will be able to utilise all of the investigative powers provided for under the Privacy Act, including the power to conduct an own motion investigation[29], in relation to health information in consumers' PCEHRs. However, s 73 of the PCEHR Bill refers particularly to s 36 of the Privacy Act, which relates to the Commissioner's power to investigate a complaint made by an individual[30], when discussing the Information Commissioner's powers.[31] In the absence of an express provision in the PCEHR Bill it may leave open to question whether the Information Commissioner can conduct own motion investigations for possible contraventions of the PCEHR Bill in circumstances where a complaint has not been made by an individual.

The power to conduct own motion investigations will be an important component of ensuring comprehensive privacy oversight of the PCEHR System, particularly given that the mandatory data breach notification requirements in Part 5 of the PCEHR Bill do not apply to all entities (such as healthcare provider organisations) that may collect health information from the PCEHR system.

Part V of the Privacy Act also provides the Information Commissioner with a range of powers when conducting investigations including the power to compel disclosure of information[32], examine witnesses[33], enter premises to examine documents[34] and, in relation

[28]Explanatory Memorandum to the PCEHR Bill, p 2.

[29] Section 40 (2) of the Privacy Act (in Part V).

[30] Section 36(1) of the Privacy Act states 'subject to subsection (1A), an individual may complain to the Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual.'

[31] See the Note to s 73 of the PCEHR Bill.

[32] Section 44 of the Privacy Act.

to IPP complaints, to call compulsory conferences[35]. The OAIC understands that it is intended that all of the investigative powers in Part V may be invoked by the Information Commissioner in relation to possible contraventions of the PCEHR Bill. However, this is not explicit in the PCEHR Bill and Explanatory Memorandum.

The OAIC recommends that, for greater certainty, the PCEHR Bill and Explanatory Memorandum should clarify that the Information Commissioner can invoke all the investigative powers provided under Part V of the Act, including own motion investigations.

The OAIC also recommends amending the Privacy Act to confirm that the Information Commissioner may investigate anyone who may have contravened a civil penalty provision in the PCEHR Bill. At present, s 73[36] of the PCEHR Bill, which makes a contravention under the PCEHR Bill an interference with privacy under the Privacy Act, may not be consistent with existing wording in Part V of the Privacy Act.[37] For example, Part V of the Privacy Act repeatedly refers to a 'respondent' to a complaint. However, the definition of 'respondent' does not extend to State or Territory authorities or other entities that are currently exempt under the Privacy Act.[38] Another issue is that the Privacy Act generally does not apply to acts of individuals except in specific circumstances.

In the OAIC's view, if the regulation of State and Territory authorities (and others not currently covered by the Privacy Act) is not established appropriately, the Information Commissioner's power to investigate possible contraventions of the PCEHR Bill may be limited. As a useful guide, reference could be made to s 27A of the Privacy Act, which was enacted for the purposes of the HI Act.

The Independent Advisory Council

In principle, the OAIC supports the establishment of an Independent Advisory Council, with the function of advising the System Operator including on privacy matters relating to the operation of the PCEHR system.[39] The OAIC understands that it is a requirement that at least one of the members appointed to the Council has experience or knowledge of matters

[33] Section 45 of the Privacy Act.

[34] Section 68 of the Privacy Act.

[35] Section 46 of the Privacy Act.

[36] Section 73 of the PCEHR Bill states that 'An act or practice that contravenes this Act in connection with health information included in a consumer's PCEHR, or would contravene this Act but for a requirement relating to the state of mind of a person, is taken to be: (a) for the purposes of the Privacy Act, an interference with the privacy of the consumer; and (b) covered by section 13 or 13A of that Act, as applicable'.

[37] See s 6C of the Privacy Act.

[38] See ss 36(6) to (8) of the Privacy Act.

[39] Section 24(2)(a) of the PCEHR Bill.

including 'law and/ or privacy'.[40] Given the importance of privacy in establishing and maintaining public confidence in the system, the OAIC submits that this could be amended to ensure that at least one member of the Council has experience or knowledge of privacy. This could be distinct from the requirement that at least one member have experience or knowledge of law.

Complaints Handling

The PCEHR Bill specifies that one of the functions of the System Operator is to establish a mechanism for handling complaints about the operation of the PCEHR system.[41] No further description of the complaints handling regime is provided for in the Bill. The Explanatory Memorandum describes that the complaint handling mechanism will provide national arrangements for consumers and participants to make complaints with other appropriate bodies such as national or state privacy health information regulators.[42]

The PCEHR Bill (or at a minimum, the PCEHR Rules) should clarify the complaints handling process that applies in relation to privacy complaints. In particular, the Bill should clarify:

- Whether an individual will generally be required to have complained to the respondent before making a complaint to the System Operator or privacy regulator. Under the Privacy Act, the Commissioner has discretion to decline to investigate a complaint where an individual has not complained to the respondent or to defer investigating a complaint while the respondent completes their investigation, unless the Commissioner decides it is not appropriate for the complainant to complain to the respondent.[43]
- The process for referring complaints, including from the System Operator to a privacy regulator, and from one privacy regulator to another;
- Whether when referring a complaint, the System Operator and privacy regulators will be authorised to provide material relevant to the complaint to the other regulator.

The OAIC also recommends that the PCEHR Rules should provide that any complaint handling regime established by the System Operator ensure that all complaints are captured by the System Operator to enable comprehensive complaint reporting and evaluation.

[40] Section 27(2)(b)(iii) of the PCEHR Bill.

[41] Section 15(j) of the PCEHR Bill.

[42] Explanatory Memorandum to the PCEHR Bill, p 15.

[43] See s 40(1A) and s 41(2)(b) of the Privacy Act.

Data Security

The OAIC supports the inclusion of data breach notification provisions and prescribed purposes for which consumers' information can be collected, used and disclosed in the PCEHR Bill. However, it is similarly important for organisations handling personal information to have appropriate security protections in place to limit the risk of a data breach.

The OAIC recommends that data security provisions which would apply uniformly to the System Operator, portal operators and repository operators should be imposed. Such a provision could be modelled on National Privacy Principle 4.1 in Schedule 3 of the Privacy Act. This provision states that 'an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure'. Section 27 of the HI Act could also be used as a model.

The OAIC considers that imposing a positive, consistent data security requirement would reinforce the importance of protecting the security of individuals' health information, in circumstances where different privacy laws may otherwise apply. It could also form the legislative basis for an appropriate civil penalty provision for serious breach of data security requirements to apply uniformly across all jurisdictions, ensuring that individuals throughout Australia have access to the same protections.

A data security requirement provision is also important given that s 75 of the PCEHR Bill, which requires certain participants in the PCEHR System to notify data breaches, only applies where an entity becomes 'aware' of data breach or possible data breach. The absence of a consistent data security obligation could make it difficult to assess the circumstances in which a participant could or should reasonably have been aware of a data breach.

The OAIC notes that the National E-Health Transition Authority (NEHTA) has developed the National eHealth Security and Access Framework, which is will give 'the health sector a common approach and language for the protection of patient information in Australia and provide further comfort to people concerned about their privacy'.[44] The OAIC supports this development. However, the OAIC reiterates the importance of implementing data protection provisions within the legislation to complement the security and access framework and further strengthen the data security arrangements.

[44] See: http://www.nehta.gov.au/media-centre/nehta-news/942-nehta-releases-ehealth-information-security-and-access-framework-to-strengthen-patient-records-protection

Civil Penalties and other Remedies

Data Breach Notifications

The OAIC recommends that the PCEHR Bill should clarify the Information Commissioner's power to investigate a possible contravention of the civil penalty provisions, where the contravention is not in connection with a consumer's health information.

Under the PCEHR Bill, if an entity fails to notify the Information Commissioner of a data breach, and the data breach is not 'in connection with a consumer's health information included in a registered consumer's PCEHR', the Information Commissioner may not have the power to investigate certain contraventions of the PCEHR Bill. This situation may arise in circumstances where the contravention is in relation to an individual's 'identifying information' rather than 'in connection with a consumer's health information'. This may affect the Information Commissioner's decision as to whether to seek a remedy in relation to contravention(s) of civil penalty provisions.

Further, the data breach notification requirements will only apply to the System Operator, registered repository operators and registered portal operators, and not to other entities which may access consumers' health information from the PCEHR system. This limitation raises a number of concerns. Firstly, the System Operator may not become aware of a data breach (or potential data breach) known to a healthcare provider organisation, such as a large general practitioner practice, at the earliest possible time. Consequently, the System Operator may not be able to appropriately respond to a breach. Additionally, it may create an unintended gap in the comprehensive protection of PCEHR information and risk lowering consumer confidence in the handling of their information in the PCEHR System.

For those reasons, the OAIC recommends that consideration should be given to extending the application of the data breach notification requirements to all entities accessing the PCEHR System.

Unauthorised use and disclosure

The OAIC recommended, in its submission to DoHA on the Draft Bill, that consideration be given to the scope and implications of the exemption in s 52 of the exposure draft PCEHR Bill. Section 52 provided that the civil penalty provisions in Part 4 of the Draft Bill would not apply to health information that was originally obtained from the PCEHR system, where such information was 'stored in such a way that it was capable of being obtained other than by means of the PCEHR system', and 'that information was obtained by those other means'. In the PCEHR Bill, this exemption has been deleted and a new provision included.[45]

[45] Section 71(1) of the PCEHR Bill.

However, in the OAIC's opinion, these provisions have a similar effect to the exemption in s 52 of the exposure draft PCEHR Bill.

The Explanatory Memorandum provides that the privacy regime in the PCEHR Bill is not intended to cover the field in relation to the 'collection, use or disclosure of health information outside the PCEHR system, or in a manner that does not use the PCEHR system, unless the contrary intention appears'.[46] This seems to imply that information downloaded from the PCEHR system and stored in a local system is considered to be outside the PCEHR system (despite being derived from the PCEHR system) and therefore will not be subject to the civil penalty provisions set out in Division 1 of Part 4 of the PCEHR Bill. Instead, any existing privacy and health laws will apply depending on the jurisdiction. However, for some entities, there may be no privacy law applying to consumer's health information once it is downloaded from the PCEHR system (for example, state healthcare provider organisations operating in a State where no privacy laws apply).

In the OAIC's opinion, individuals have an interest in clear and consistent privacy protections applying to their health information in the PCEHR system, irrespective of where it is accessed and how it is subsequently stored. This is particularly important given that the PCEHR system will transform the way in which health information is shared across jurisdictions, making it much easier for individuals' health information to be transferred between healthcare providers.[47]

The OAIC recommends that the protections embedded in the PCEHR System by the legislation should apply to all health information within the System including information that was originally obtained from the PCEHR system and later stored elsewhere.

'Identifying Information' and 'Healthcare Identifiers'

The OAIC recommends that the Senate Committee seek clarification of whether 'identifying information' and 'healthcare identifiers' handled under the new Division 2A, Part 3 of the *Healthcare Identifiers Act 2010 (Cth)* (HI Act), would be covered by the civil penalty provisions in Division 1, Part 4 of the PCEHR Bill. The OAIC notes that the PCEHR Bill has included a separate definition of the term 'identifying information' at s 9. However, it remains unclear whether, once this information is included in the PCEHR System, this information is covered by the definition of 'health information' in the s 5 of the PCEHR Bill, such that if it were inappropriately collected, used or disclosed, the civil penalty provisions in Division 1, Part 4 of the PCEHR Bill would apply.

[46] Explanatory Memorandum to the PCEHR Bill, p 39.

[47] OAIC, Submission to DoHA on the *PCEHR System: Legislation Issues Paper*, p. 14

Remedies

The OAIC recommends that further consideration should be given to the remedies available in the PCEHR Bill to ensure that there is an appropriate remedy where an entity, such as a registered healthcare provider organisation, breaches a PCEHR Rule.

The OAIC understands that it is intended that the PCEHR Rules will cover important aspects such as registration requirements including technical specifications, access control mechanisms and authorised representatives and nominated representatives.[48] These are important matters that impose requirements on all participants about how information within the PCEHR System should be handled. The Explanatory Memorandum provides that a failure to comply with a relevant requirement in the PCEHR Rules may result in cancellation or suspension of a participant's registration and/ or other sanctions, including the imposition of a civil penalty[49]. However, the imposition of civil penalties for breaches of a PCEHR Rule are limited to registered repository operators or registered portal operators. It seems that not all participants, as defined in s 6 of the PCEHR Bill, will be subject to civil penalties for breach of a PCEHR Rule.

Accordingly, the OAIC recommends that all participants should be subject to civil penalties for breaches of the PCEHR Rules.

PCEHR Rules

The OAIC notes that under s 109 of the PCEHR Bill the Minister *may*, by legislative instrument, make rules called the PCEHR Rules. The OAIC recommends that the making of the PCEHR Rules should be mandatory under the PCEHR Bill.

There are a number of matters to be included in the PCEHR Rules which will be integral to ensuring appropriate privacy protections are available for consumers (in addition to those mentioned earlier), such as physical and information security and default access controls. If the PCEHR System becomes operational prior to the Minister making PCEHR Rules or in the absence of the Minister making such Rules, this may pose a privacy risk for consumers' health information contained in the PCEHR System.[50]

Definitions

The OAIC recommends the Senate Committee seek clarification of the reasons for using the terms 'collecting' health information and 'obtaining' health information and any

[48] Section 109, PCEHR Bill.

[49] Explanatory Memorandum to the PCEHR Bill, p 60.

[50] For example see s 15 of the *Intelligence Services Act 2001.*

implications of using these different terms. Section 52 of the Draft Bill, which referred to 'obtaining health information', has been removed. However, s 71 of the PCEHR Bill, which relates to prohibitions and authorisations limited to the PCEHR System, also refers to 'obtaining health information' as distinct from 'collecting health information'. The Explanatory Memorandum does not clarify whether there are any implications from the use of these different terms. The OAIC recommends that the PCEHR Bill apply consistent terminology to avoid confusion.

Reporting and Review of the PCEHR Bill

Reporting

The OAIC recommends that all privacy regulators should be required to compile and report their statistics about complaints received and investigations undertaken in relation to PCEHRs or the PCEHR system.

The PCEHR Bill only requires the Information Commissioner to compile and report on statistics in relation to the PCEHR system. This means that complaints made directly to state or territory privacy regulators may not be included in the PCEHR reporting. Consequently, the volume of privacy complaints handled in relation to the PCEHR system may not be accurately represented. Accurate statistics will be important in ensuring an effective review of the PCEHR system. The OAIC recommends that state and territory privacy regulators should be required to report their statistics about complaints received and investigations undertaken in relation to PCEHRs or the PCEHR system to the OAIC.

Review

The OAIC recommended that review under s 96 of the Draft Bill should also include an assessment of the adequacy of privacy protections under the PCEHR legislation. The OAIC also recommended that review should involve consultations with a wide cross-section of the community in relation to the adequacy of privacy protections.

The OAIC notes that s 108(4) of the PCEHR Bill now requires the person undertaking review to 'call for and consider submissions from members of the public'. However, the OAIC maintains that the PCEHR Bill should also specify that the consultation must consider the adequacy of privacy protections.

PCEHR (Consequential Amendments) Bill

The Consequentials Bill inserts a new Division 2A in Part 3 of the HI Act. Division 2A will authorise the System Operator, registered repository operators and portal operators to collect, use and disclose healthcare identifiers (as defined in the HI Act). Further, the System Operator will also be able to collect, use and disclose healthcare identifiers and identifying

information (as defined in the HI Act) in certain circumstances.[51] The System Operator, repository operators and portal operators may collect, use and disclose this information including for 'purposes of the PCEHR system, subject to the *Personally Controlled Electronic Health Records Act 2011*.'[52]

In the OAIC's view, these provisions do not make sufficiently clear the particular purpose/s for which operators may collect, use or disclose this information. If the HI Act does not describe such purpose/s more clearly, operators may be able to decide whether a collection, use or disclosure is appropriate in the circumstances. This in turn, could lead to inconsistent information handling practices by operators, which may not reflect consumers' expectations.

The OAIC therefore recommends that the Consequentials Bill specify more clearly the particular purpose for which operators may collect, use or disclose this information. The OAIC recommends that this could be established by clearly setting out the circumstances in which operators may collect, use and disclose this information and by limiting the allowable purposes to the functions prescribed under the PCEHR Bill.

[51] See clause 21 in Schedule 1 of the Consequential Amendments Bill (which inserts a new s 22A and s 22C in the HI Act).

[52] See clause 21 in Schedule 1 of the Consequential Amendments Bill (which inserts a new s 22A(2) and s 22C in the HI Act).