Australian Government

Office of the Australian Information Commissioner

Health Legislation Amendment (eHealth) Bill 2015

Submission to Senate Community Affairs Legislation Committee

October 2015

Timothy Pilgrim, Acting Australian Information Commissioner

Contents

Introduction

Thank you for providing the Office of the Australian Information Commissioner (OAIC) with the opportunity to comment on the *Health Legislation Amendment (eHealth) Bill 2015* (the Bill). The OAIC understands that the primary purpose of the Bill is to make changes to the personally controlled electronic health record (PCEHR) system, including changes to facilitate the trial and possible future expansion of an opt-out model of participation.

The OAIC recognises the benefits that are expected to accompany an effective eHealth record system in Australia. These benefits include better health outcomes arising from the improved availability and quality of health information, fewer adverse medical events, and procedural and economic efficiency through reduced duplication of treatment.

However, changes to the current PCEHR system do raise potential privacy issues. The system is expected to increasingly handle significant volumes of sensitive health information. In addition, the Bill provides for the conduct of trials of an opt-out model of participation, with the possibility of that model being expanded nationally in the future. Under opt-out arrangements, the health information of a healthcare recipient who does not opt-out will be handled in the PCEHR system without that individual's express consent. In addition, a healthcare recipient's knowledge about the arrangements will be dependent upon an effective awareness campaign.

In the context of an opt-out system, it is important to provide healthcare recipients with control over if and how their health information is handled, and to ensure strong privacy protections are in place for those who do not choose to opt-out. The OAIC considers that strong privacy safeguards should be a critical aspect of an eHealth system operated on an opt-out basis. Ensuring that privacy is adequately addressed and protected is also fundamental to establishing and maintaining public confidence in the system.

The OAIC acknowledges that the PCEHR Act (as it would be amended by the Bill) sets out safeguards for privacy, such as providing for healthcare recipients to opt-out, and allowing for healthcare recipients to advise healthcare providers not to upload particular documents. The PCEHR Act also provides for appropriate oversight by requiring participants in the PCEHR to notify data breaches to the Information Commissioner and the System Operator and providing for consumer notification, and by providing the Information Commissioner with a range of regulatory functions and enforcement powers. In addition, the OAIC acknowledges that the Explanatory Memorandum to the Bill notes the Department's intentions in relation to other safeguards including the opt-out process and a related public awareness campaign. The OAIC welcomes these statements.

However, the OAIC believes that the Bill in its current form raises a number of privacy issues that warrant further consideration. The comments below are primarily aimed at analysing the privacy implications of changing to an opt-out model, and identifying the main areas where further consideration or clarity is required to ensure that the privacy impacts of a number of legislative changes proposed in the Bill are minimised.

The OAIC's eHealth regulatory role

The OAIC is the independent regulator of the privacy aspects of the personally controlled electronic health records (PCEHR) system and the Healthcare Identifiers (HI) service. The OAIC has performed these regulatory roles since those systems commenced in 2012 and 2010 respectively.

The privacy framework for the PCEHR system and HI Service is currently set out in the *Privacy Act 1988,* the *Personally Controlled Electronic Health Records Act 2012* and the *Healthcare Identifiers Act 2010*. The OAIC has a range of regulatory functions and enforcement powers under both the Privacy Act and PCEHR Act to ensure compliance with these privacy requirements.

In addition, the OAIC has entered a Memorandum of Understanding (MOU) with the Department of Health in relation to the OAIC's delivery of independent regulatory services in relation to both the PCEHR system and HI service.[1] In addition to exercising the regulatory and enforcement functions mentioned above, the OAIC also performs a number of other activities under this MOU. This includes responding to enquiries and requests for advice on eHealth privacy compliance obligations, and developing written guidance materials on privacy for users of the system. The OAIC's full range of eHealth regulatory activities is set out in the MOU.

An 'opt-out' participation model for the PCEHR system

The PCEHR system has operated since its 2012 commencement under an 'opt-in' model where PCEHRs are only created for those healthcare recipients who actively register for the system. The Bill contains provisions which, if enacted, will allow for the trial of an 'opt-out' participation model, followed by a possible expansion of that model nationally.

The OAIC has supported the use of an opt-in participation model for Australia's eHealth record system.[2] From a privacy perspective, using an opt-in model provides a higher degree of privacy protection as it gives healthcare recipients the ability to decide upfront whether or not to participate. This means healthcare recipients have provided active and express consent before they are registered in the system and their health information is uploaded to their record.

While an opt-in model gives health recipients this initial level of control, the OAIC understands that, in response to the recommendations of the review of the PCEHR,[3] the Australian Government has decided to trial the use of an opt-out participation model

---

1 The current Memorandum of Understanding between the Department of Health and the OAIC is available at: http://www.oaic.gov.au/about-us/corporate-information/mous/mou-between-department-of-health-and-oaic-june-2015.

2 For example, see http://www.oaic.gov.au/engage-with-us/submissions/draft-concept-of-operations-relating-to-the-introduction-of-a-personally-controlled-electronic-health-record-pcehr-system#_Toc295919481, and http://www.oaic.gov.au/engage-with-us/submissions/electronic-health-records-and-healthcare-identifiers-legislation-discussion-paper#s3-3-1-an-opt-out-pcehr-system.

3 The report from the review of the PCEHR is available here: http://health.gov.au/internet/main/publishing.nsf/Content/ehealth-record.

ahead of making a final decision as to whether the opt-out approach should be adopted nationally. Under an opt-out model, an eHealth record is created for each healthcare recipient unless that individual has taken active steps to opt-out of the system.

While the OAIC is aware of the policy reasons behind the Government's proposal to trial an opt-out model, the OAIC notes that this change in approach does increase the privacy risks faced by healthcare recipients. In particular:

- a healthcare recipient's health information will be handled for the purposes of the PCEHR system without that individual's express consent. This does not align with best privacy practice, which generally involves obtaining express consent before handling health or other sensitive information given the bigger privacy impact that handling this type of information can have
- within a short period of time, an opt-out system will result in an increasing volume of health information being more readily available and to more people than has previously been possible. This creates an increased risk of privacy incidents such as the inadvertent disclosure or misuse of health information. Given that health information is of a particularly sensitive nature, the consequences of these incidents can be more serious.

Given the increased privacy risks, a decision to adopt an opt-out model is significant and it is important that it is implemented in the most privacy-enhancing way possible. For this reason, the OAIC supports the proposal reflected in the Bill to conduct trials of an opt-out model before adopting such a model nationally. Trialling the approach, carefully evaluating the outcomes, and using these outcomes to inform legislative and procedural adjustments will be important for ensuring that any nationally-applied opt-out model is implemented in as privacy-enhancing a way as possible.

In addition to the conduct of trials, additional essential privacy safeguards are needed (both during the trials and subsequently) to ensure healthcare recipients are likely to know how their health information is being handled, and can exercise their right to opt-out. This means that the opt-out process must be accessible and easy to use, and there must be an effective public awareness campaign about the opt-out PCEHR system and the opt-out process. More detail about these important safeguards is set out below.

Opt-out process and public awareness campaign

Two important privacy safeguards that must accompany an opt-out model are a fair and easy to use opt-out process, and an effective public awareness campaign about the PCEHR system and a healthcare recipient's options for controlling how their personal information is handled.

Under an opt-out model, the PCEHR System Operator will no longer need to obtain healthcare recipients' express consent to participate in the system as the registration of healthcare recipients and the uploading of records will be authorised by law. However, to mitigate the privacy impacts and give healthcare recipients choice and control over how their personal information is handled, the System Operator nevertheless should try to obtain healthcare recipients' implied consent by giving them an adequate opportunity to

opt-out of the system. The opt-out process and the public awareness campaign are critical to achieving this.

Healthcare recipients should be provided with effective communication about the system and their right to opt-out. To achieve this, the public awareness campaign should satisfy the following criteria:

- it should provide sufficient information to enable healthcare recipients to understand what the PCEHR system is and the benefits and risks of participation, and to understand what their options are
- the option to opt-out of the system should be clearly and prominently presented
- the campaign needs to be of sufficient scope so that it is likely that each affected healthcare recipient has received and read the information about the PCEHR system, the option to opt-out, and the opt-out process
- the information provided for healthcare recipients should clearly explain the implications of not opting-out. This information should also clearly explain the personal controls available to them, when they will become available and how they can be set
- the material should be accessible, written in plain English and should also be provided in ways that take into account the needs of healthcare recipients with particular needs, such as those from a non-English speaking background and disadvantaged or vulnerable individuals.

In addition, the opt-out process must be fair and easy to use. This includes:

- allowing healthcare recipients an adequate time period in which to receive and consider information about the opt-out system, to make their decision about whether or not to opt-out, and to exercise their right to opt-out if they so choose
- providing free, simple and accessible means of opting-out of the system, including means that take account of the needs of healthcare recipients with particular needs.

The OAIC welcomes statements in the Explanatory Memorandum that note an intention to conduct an appropriate awareness raising campaign in relation to an opt-out model, and acknowledge that stakeholder consultations revealed a firm view that strong and effective communication would be needed in relation to the privacy implications of moving to an opt-out model.[4] In relation to the opt-out process, the Explanatory Memorandum also notes that the process is intended to be simple, that healthcare recipients will be given a reasonable opportunity to opt-out, and that various opt-out channels are being developed.[5]

However, the OAIC notes that the Bill and the Explanatory Memorandum provide little specific detail about how this awareness campaign will be conducted, or the timing of the opt-out process. Given the importance of these safeguards, the OAIC recommends that

[4] For example, see Explanatory Memorandum pp 9, 25 and 94.
[5] See Explanatory Memorandum p 94.

the Bill and/or the Explanatory Memorandum be amended to provide clearer requirements and detail about the parameters of these privacy safeguards and how they will be implemented. In addition to providing clarity, this will help to ensure the safeguards are applied consistently, and will increase public confidence in an opt-in system.

For example, the OAIC notes that the Department of Health had earlier indicated an intention for a staged process to opting-out where healthcare recipients included in an opt-out trial would be given a two month period to opt-out, followed by a six week period for setting access controls before healthcare providers can access the records.[6] The OAIC supported this proposal, and considers those periods to be appropriate timeframes to trial. This is an example of specific detail that could be included in the Bill and/or the Explanatory Memorandum to ensure that appropriate privacy safeguards are in place.

Under the OAIC's MOU arrangement with the Department of Health, the OAIC has a role in liaising on privacy-related PCEHR activities with the PCEHR System Operator and other key agencies, and to comment on eHealth developments that relate to the PCEHR system. Given this role and the OAIC's expertise in privacy, the OAIC is very willing to be consulted on the proposed plans and draft communication materials for the public awareness campaign. Similarly, the OAIC is willing to assist in the evaluation of the privacy impacts of the trial and the update of awareness materials if opt-out is subsequently expanded nationally.

Personal control

Healthcare recipients being able to exercise personal control over their PCEHR has been an important privacy safeguard in the current PCEHR system. The availability of access and other personal controls takes on even more importance in the context of an opt-out system given that a healthcare recipient's express consent to the handling of their personal information has not been obtained.

It is therefore important to ensure that existing access and other personal controls are not diminished. With the exception of the upload of health information held by Medicare (see below), the OAIC understands that existing controls will continue to be available. This includes the ability for healthcare recipients to control which health providers can access their record, and ability to expressly request that a healthcare provider not upload a particular document. There is also a new control where healthcare recipients can choose to be notified when their PCEHR is opened or used.

Given that, by default, these controls are not activated, it is important that sufficient information about the controls is available to healthcare recipients. That information must ensure that recipients can understand what controls are available, the consequences of setting or not setting a particular control, and how to go about setting controls. In addition, the process for setting controls should be accessible and simple for

[6] See pp 13-14 of the *Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper* at https://consultations.health.gov.au/ehealth/ehr-and-hi-legislation-discussion-paper-1.

all sections of the community, and an adequate period for setting controls should be available before healthcare providers gain access to records.

Upload of Medicare information

Under the current opt-in model, healthcare recipients have the choice to consent (or not consent) at the time of registration to the upload of health information held by DHS Medicare, including Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) claims information (s 38(2)(b)). MBS and PBS information can indicate diagnosed conditions and illnesses. Healthcare recipients are currently advised of this risk when deciding whether or not to consent to the upload of this information, and this is an important privacy safeguard and aspect of personal control under the current model.

Under the opt-out model proposed in the Bill, healthcare recipients will no longer be asked to expressly consent to the upload of this information. Rather, the Chief Executive Medicare is authorised to upload the information, unless the healthcare recipient has taken steps to actively notify the Chief Executive Medicare not to upload the information (Item 106, clauses 12-13).

This is a reduction in the privacy protection afforded to this information. The OAIC recommends that the public awareness campaign clearly inform healthcare recipients about how their Medicare information will be handled and their options, and that this information may include detail that indicates diagnosed conditions and illnesses.

Expansion of opt-out following trials

Under the Bill, the Minister will be able to make My Health Records Rules applying the opt-out model to a class, or classes, of healthcare recipients who will participate in trials of an opt-out model (item 106, clause 1). In addition, the Bill proposes to allow the Minister to make My Health Record Rules expanding the opt-out model nationally if the Minister decides, based on the trials, that the opt-out model 'provides value' (item 106, clause 2). Before applying the opt-out model nationally, the Minister must consult with the Ministerial Council.

A decision to apply the opt-out model nationally would be a significant change in the handling of health information for the purposes of the PCEHR system, and raises potential privacy issues as outlined in this submission. While the trials may allow some of these issues to be mitigated before a national roll-out, the decision would still be significant, particularly given the sensitivity of the information handled in the PCEHR system. The OAIC therefore recommends that consideration be given as to whether it is appropriate for this decision about the future direction of the PCEHR system to be made by rules rather than being made by Parliament and effected by change to the primary legislation.

If the ability for the Minister to make this decision via the My Health Record Rules is retained, then the OAIC notes that it is important that the trials are thoroughly evaluated and that the learnings relevant to privacy are taken into account. The trials are intended

to gather evidence to improve the system, including in relation to privacy.[7] Therefore, for the trials to operate as an effective privacy safeguard as intended, any areas for improvement identified during the trials should be addressed and any necessary legislative changes made. The OAIC recommends that consideration be given to alternative approaches that would more clearly ensure that privacy is taken into account in this decision, such as:

- changing the wording of item 106, clause 2(2) to require the Minister to consider the privacy impacts in the Minister's decision whether to apply the opt out model to all healthcare recipients in Australia
- requiring the Minister to engage in consultation more broadly than with just the Ministerial Council (as currently envisaged by (3)), including specifically with the Australian Information Commissioner.

In addition, before any decision is made to apply the opt-out model nationally, the OAIC recommends that the Minister arranges for an independent privacy impact assessment (PIA) to be conducted to identify, evaluate and address privacy risks that arise during the trials.[8] Given its regulatory oversight role in relation to the system, and the OAIC's MOU with the Department, the OAIC would expect to be consulted on the draft PIA.

Mandatory data breach notification

Section 75 of the PCEHR Act creates a mandatory data breach notification (MDBN) obligation for certain participants in the PCEHR system. The Bill proposes to amend s 75 to extend the existing MDBN obligation to all registered healthcare provider organisations and registered contracted service providers. This change significantly expands the scope of this MDBN scheme.

The OAIC is generally supportive of the extension of MDBN obligations to all participants in the PCEHR system. The OAIC considers that an effective MDBN scheme can provide a strong incentive for participants to establish and maintain appropriate information handling practices and data security protections.

However, the OAIC has two concerns that flow from the particular notification thresholds that are proposed, and believes that further consideration should be given to the appropriate notification threshold for this expanded MDBN scheme.

Firstly, the OAIC notes that the Australian Government is currently considering a general MDBN scheme. A general scheme could, if adopted, apply to many of the entities who will also be subject to the PCEHR MDBN scheme. The OAIC therefore believes that the PCEHR MDBN obligations need to be considered in the context of any general MDBN scheme. The OAIC considers that the ideal approach would be to have one test that

[7] See Explanatory Memorandum p 91.

[8] For more information on conducting PIAs, see the OAIC's Guide to undertaking privacy impact assessments: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments.

applies to all MDBN (whether PCEHR-related or not). That test should include a 'seriousness' threshold, such as a real risk of serious harm to affected individuals.

The OAIC's concern about potentially having two schemes with different reporting thresholds relates to the regulatory complexity that this may create. This is particularly the case for private sector healthcare providers who may be subject to PCEHR Act MDBN requirements in relation to their use of the PCEHR system, and subject to another set of requirements in relation to other health information they hold. This problem may be exacerbated by the fact that it is not always easy for providers to determine in practice what information is part of the PCEHR and what is outside the PCEHR, leading to confusion about reporting requirements.

The OAIC's second concern relates to the proposed threshold in the Bill under new s 75(6) for notifying healthcare recipients of breaches (as opposed to notifications to the OAIC or System Operator). The effect of this provision is that for all data breaches, all affected healthcare recipients must be notified, with no consideration being given to the seriousness of the breach or the risk posed to those healthcare recipients. While healthcare recipient notification is an important mitigation strategy following some breaches, in other low-risk situations, it is less appropriate and may cause undue anxiety for those who receive notifications. In addition, the frequent receipt of notifications can lead to 'notification fatigue', whereby individuals no longer take notifications seriously. The result is that when a particular breach presents a high risk of harm to those individuals, they may not take the necessary action to protect their privacy which they would otherwise have taken if notifications were less frequent and only sent in relation to more serious breaches. For this reason, the OAIC believes that the proposed threshold in new s 75(6) may inadvertently undermine privacy protection.

While the Bill could continue to require these events and circumstances to be notified to the Information Commissioner and/System Operator for transparency and monitoring of the system, the OAIC is concerned about the possibility of healthcare recipient notification fatigue if frequent notifications occur. The OAIC therefore recommends that a higher threshold for healthcare recipient notifications be adopted in 75(6), similar to that in s 75(5).

New regulation-making powers

Item 34 of the Bill proposes to add to the *Healthcare Identifiers Act 2010* new ss 20 and 25D which are regulation-making powers. Proposed s 20 would allow regulations authorising the collection, use, disclosure and adoption of the identifying information and healthcare identifiers of healthcare recipients for purposes related to the categories outlined in s 20(3), which broadly relate to the provision of 'healthcare' and to 'assisting person who…require support'. Section 25D is in similar terms, but relates instead to the handling of identifying information and healthcare identifiers of healthcare providers.

The OAIC understands that the purpose of these new provisions is to allow the range of entities that can handle healthcare identifiers to be expanded as required (within the limits of ss 20(3) and 25D(3)) without needing to amend the legislation. The powers

would also allow additional collections, uses and disclosures of healthcare identifiers to be prescribed.

Allowing the way healthcare identifiers are handled and used, and the entities authorised to handle them, to be expanded via regulation risks allowing function creep over time. The OAIC recommends that any such regulation-making power be narrowly drafted to minimise this risk.

While subparagraphs (3)(a), (b), (c) and (e) limit this regulation-making power to purposes related to healthcare and the My Health Record system, the OAIC is concerned that (d) – 'assisting persons who, because of health issues (including illness, disability or injury), require support' – is not drafted narrowly enough to avoid this risk. The OAIC recommends that the phrase 'require support' be qualified by a reference to 'healthcare'. If not limited in this way, this subparagraph could be used to expand the handling of healthcare identifiers beyond the original intention behind healthcare identifiers of matching health information to individuals when healthcare is delivered.[9] This is because people who have health issues might 'require support' to access any number of services whether those services are related to healthcare or not. If there are particular non-healthcare provider entities which (d) is intended to capture (such as the National Disability Insurance Agency and cancer registers mentioned in the Explanatory Memorandum), then the OAIC additionally recommends that these authorisations instead be specified in the legislation.

Given the privacy risks associated with unique identifiers such as healthcare identifiers, it is important that any expansion in the handling of healthcare identifiers is subject to sufficient consultation and scrutiny. The OAIC therefore recommends that proposed ss 20 and 25D be amended to require the Department to consult with stakeholders in the making of the regulation, including a specific requirement that the Information Commissioner be consulted, before making such regulations. In addition, given the possible impact on privacy that regulations under these provisions could have, the OAIC recommends that the Government undertake a PIA before prescribing additional entities and uses under these sections. A PIA would ensure that the privacy risks of a particular expansion are identified, and that steps are taken to eliminate, minimise or manage those risks.

[9] Section 3 of the *Healthcare Identifiers Act 2010* notes that *'The purpose of this Act is to provide a way of ensuring that an entity that provides, or an individual who receives, healthcare is correctly matched to health information that is created when healthcare is provided. This purpose is to be achieved by assigning a unique identifying number to each healthcare provider and healthcare recipient.'*

Other privacy issues

Privacy Act definition of 'health service'

Item 109 of the Bill proposes to insert s 6FB into the *Privacy Act 1988* (Cth), which provides a new definition of 'health service'.

Subsection 6FB(4) allows the regulations to prescribe an activity that is not to be treated as a health service for the purposes of the Privacy Act. Given the OAIC's expertise and experience in applying this definition in the context of its regulatory activities, the OAIC recommends that this section be amended to include a specific requirement that the Information Commissioner be consulted in the making of any regulation under this section.

Retention of records in the National Repositories Service

Section 17 of the PCEHR Act currently provides that records held in the National Repositories Service (NRS) must be retained until either 30 years after the healthcare recipient's death, or 130 years after the record was first uploaded if the date of death is unknown. The OAIC notes that Item 71 of the Bill proposes to amend s 17 so that where the date of death is unknown, the record must be retained for 130 years from the healthcare recipient's date of birth.

While the OAIC welcomes a reduction in the time that records uploaded to the NRS must be retained, the OAIC does query whether the length of the retention period is necessary. A shorter retention period would be consistent with APP 11, which states that where an entity holds personal information it no longer needs for a purpose permitted under the APPs, it must take reasonable steps to destroy or de-identify the information (APP 11.2). A shorter retention period would better align with the destruction timeframes that apply to the majority of Commonwealth records as regulated under the *Archives Act 1983* (Cth).

The OAIC recommends that consideration be given to whether the clinical and other authorised purposes would be satisfied if records are retained for a shorter period. Also, consideration should be given to whether holding records for that period is necessary and proportionate to those purposes.

Dealing with eHealth records at the conclusion of trials

If no decision is made to extend the opt-out model nationally, the Explanatory Memorandum notes that a healthcare recipient registered under Schedule 1 will continue to have a record (including after the trials have finished) unless they cancel their registration under s 51 of the Act.[10]

The OAIC recommends that, to ensure healthcare recipients have an understanding of how their record is being handled, trial participants are notified at the conclusion of the trial. That notification should indicate that the trial has ended, that the Government has decided not to continue the opt-out approach, and should identify the healthcare

[10] See Explanatory Memorandum p 92.

recipient's options for their record. If records are to continue unless cancelled, the notice should explain this and provide cancellation instructions. An alternative option for consideration is cancelling records within a certain number of days of the healthcare recipient receiving a notice unless the recipient takes steps to keep the record active. The OAIC recommends that the Explanatory Memorandum be updated to reflect these details.

Pseudonymous records

Healthcare recipients can register for the current PCEHR system using a pseudonym. This is an important privacy-enhancing feature that allows recipients who wish to participate in the system to do so using a pseudonym.

Neither the Bill nor the Explanatory Memorandum addresses how healthcare recipients who wish to obtain such a record would do so under an opt-out system. It is also not clear how recipients who have already registered for a pseudonymous record will be impacted under an opt-out system: for example, would an identified record automatically be created for them?

The OAIC recommends that the Explanatory Memorandum be amended to acknowledge the role of pseudonymous records and to outline how such records will be addressed in the opt-out model. The OAIC also recommends that the public awareness campaign include information about the availability of pseudonymous records, and that sufficient time is allowed for recipients to register for a pseudonymous IHI before opt-out records are created. In addition, healthcare recipients who already have a pseudonymous record should be notified about how the opt-out model will affect them.

Opt-out process for minors and adults lacking capacity

An 'authorised representative' manages a PCEHR on behalf of another person because the person does not have the capacity to manage their own record. The Explanatory Memorandum makes specific reference to needing to verify that someone is an authorised representative where they are seeking to opt-out another healthcare recipient.[11] What is unclear, however, is what mechanism will be in place to ensure that, where an adult healthcare recipient who lacks capacity has not or is not opted-out, the individual has received the necessary support and information to make that decision.

In addition, where an adult healthcare recipient who is unable to manage their record is not opted-out, and the System Operator proceeds to automatically create a record for that recipient, it is unclear:

- who will manage that record and how the System Operator will ensure that the system's privacy safeguards (such as setting access controls) are genuinely available to that individual
- how the System Operator will know that the individual lacks capacity and requires an authorised representative, and how the System Operator would determine who the appropriate authorised representative should be.

[11] See Explanatory Memorandum p 97, table item 2.

A related issue arises in the case of healthcare recipients aged under 18 years who have capacity to take control of their record. It is unclear how, in the opt-out model, such individuals will be made aware of their right to take control of their record rather than leaving control of their record to their parent or legal guardian.

The OAIC recommends that the Explanatory Memorandum be amended to provide further detail on how these issues will be addressed.