



July 2017

Privacy Impact Assessment Report

My Health Record – National Opt-out Model Implementation

Prepared for the Australian Digital Health Agency



PIA Report: Contents

- 1. Executive Summary 3**
- 2. About this report 4**
- 3. Description of NOO Model 8**
- 4. Bulk registration & Opt-Out Process 11**
- 5. Ongoing opt-out registration 21**
- 6. Other privacy issues 23**
- 7. Conclusions 30**
- Schedule 1 – Detailed information flows: Bulk registration 33**
- Schedule 2 - Sources of information 48**
- Schedule 3 – Glossary and acronyms 50**



1. Executive Summary

1.1 Introduction and context

- (a) As part of the Federal Budget 2017-18, the Australian Government announced that the My Health Record system (**MHR system**) will transition from an opt-in model, to an opt-out model for individual participation on a national basis (**NOO Model**).
- (b) This PIA has been commissioned by the Australian Digital Health Agency (**the Agency**), and assesses the proposed process for the implementation of the NOO Model, specifically in relation to aspects which have changed or differ from the approach applied during the 2016 trials of the opt-out model (**Opt-Out Trials**).
- (c) Registration of healthcare provider organisations and other participants in the My Health Records system under the *My Health Records Act 2012* (**MHR Act**) will continue to be on an opt-in basis.

1.2 Summary of findings

- (a) Our recommendations are set out in full in section 7 of this report.
- (b) The key privacy risks to which our recommendations relate include ensuring that individuals:
 - (i) are adequately informed about the bulk registration process; and
 - (ii) are given sufficient opportunity to exercise their right to opt-out and set privacy controls for their My Health Record (**MHR**) before it can be accessed by healthcare providers.

2. About this report

2.1 Background

- (a) The MHR system is currently based on an opt-in participation model for healthcare recipients (i.e. individual recipients who have or may receive healthcare in Australia) and other participants in the MHR system (e.g. healthcare provider individuals and organisations).
- (b) In 2013, a review of the MHR system was undertaken by an independent panel which recommended (amongst other things) the implementation of an opt-out participation model.¹ In 2014, the Department of Health (**DOH**) commissioned Deloitte to facilitate community consultations on the recommendations of the 2013 review, which found that there was strong support amongst both consumers and clinicians for the concept of an opt-out participation model.²
- (c) In 2015, the *My Health Records Act 2012 (MHR Act)* (previously the *Personally Controlled Electronic Health Records Act 2012*) was amended to enable the Minister for Health to make My Health Records Rules to:
 - (i) implement a trial of an opt-out participation model; and
 - (ii) if the trials resulted in participation at a level that provided value for those using the system, to implement a national opt-out MHR system.
- (d) The Opt-Out Trials were conducted between March and October 2016 at sites in Northern Queensland and the Nepean Blue Mountains area of NSW. An independent evaluation of the trials commissioned by DOH was conducted by Siggins Miller Consultants to look at the outcomes from these trials.
- (e) In May 2017, the evaluation findings of the Opt-Out Trials were recently published in the *Evaluation of the Participation Trials for the My Health Record: Final Report (Evaluation Report)*. The Evaluation Report recommended that the Australian Government proceed to an opt-out MHR system, based on the report's findings that:
 - (i) the Opt-Out Trials achieved better outcomes compared to the opt-in trials in terms of participation, understanding and use;
 - (ii) an opt-out approach increased participation by both healthcare recipients and providers in the MHR system; and
 - (iii) there was a high level of support for the automatic creation of MHRs by both healthcare providers and trial participants, with an opt-out rate of 1.9 per cent across the two Opt-Out Trial sites.

2.2 Previous privacy assessments of an opt-out model

Three assessments of privacy issues and impacts relating to an NOO Model have previously been commissioned by DOH (collectively referred to as the **Previous Privacy Assessments**):

- (a) *Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model* dated 20 May 2015, prepared by MinterEllison (**2015 PIA**): This PIA analysed the personal information flows and potential privacy risks and impacts of implementing an opt-out participation model for the (then) Personally Controlled Electronic Health Record (**PCEHR**), in response to the recommendations made in the Deloitte Report.
- (b) *Privacy Impact Assessment: My Health Record – Opt-Out Trials* dated 21 March 2016, prepared by Ashurst (**2016 PIA**): This PIA related to the design of the Opt-Out Trials.

¹ Review Panel, *Review of the Personally Controlled Electronic Health Record* (December 2016).

² Deloitte, *Report to the Commonwealth Department of Health on the public consultation into the implementation of the recommendations of the Review of the Personally Controlled Electronic Health Record* (September 2014) (**Deloitte report**).

- 
- (c) *Privacy advice in relation to My Health Record Creation* dated 1 December 2016, prepared by Information Integrity Solutions for DOH (**2016 Privacy Advice**): This advice provided a high level privacy risk analysis relating to the proposed bulk transfer of information about individuals by DHS to the System Operator (NIO) before those individuals are given an opportunity to opt-out of automatic registration.

2.3 Scope of this PIA

- (a) The scope of this PIA:
- (i) is limited to information flows and aspects of the proposed NOO Model which represent material changes to the approach taken in the Opt-Out Trials, or otherwise as outlined and considered in the 2015 PIA;
 - (ii) assesses whether the proposed arrangements will:
 - (A) satisfy privacy obligations under the *Privacy Act 1988* (Cth) (**Privacy Act**), the MHR Act and the *Healthcare Identifiers Act 2010* (Cth) (**HI Act**); and
 - (B) meet community expectations about the collection, use, disclosure and protection of personal information;
 - (iii) considers:
 - (A) the planned communication strategy to inform individuals about the MHR system and the handling of their personal information under the NOO Model;
 - (B) the proposed approach to enabling individuals to exercise their right to opt-out; and
 - (C) the proposed approach to the automatic creation of My Health Records (**MHRs**); and
 - (iv) identifies and recommends options for managing, reducing or eliminating any new negative privacy impacts.
- (b) The PIA does not assess:
- (i) the MHR system as a whole, or the existing functionality of the MHR system;
 - (ii) the full range of the Agency's activities, other than those which specifically relate to the transition to and implementation of an NOO Model;
 - (iii) the myGov system generally;
 - (iv) the handling of metadata by the System Operator;
 - (v) compliance with State or Territory health legislation, privacy or secrecy laws;
 - (vi) the adequacy of security arrangements for the MHR System under an NOO Model; or
 - (vii) any testing of the MHR system before the creation of records as part of the bulk registration process.
- (c) Further, this PIA does not duplicate or re-assess the matters that have been considered, and the advice and recommendations provided in, the Previous Privacy Assessments. Recommendations made in the Previous Privacy Assessments that are relevant to the new privacy impacts identified and considered in this PIA are referenced in this report.

2.4 Methodology

- (a) To produce this PIA report, MinterEllison has:
 - (i) applied an approach based on the *Guide to undertaking privacy impact assessments (May 2014)* (**PIA Guide**) issued by the Office of the Australian Information Commissioner (**OAIC**);
 - (ii) assessed the privacy impacts of the NOO Model implementation by reference to the Australian Privacy Principles (**APPs**) in the Privacy Act, and privacy-related provisions in the MHR Act and HI Act; and
 - (iii) relied on and considered the documents and information listed in Schedule 2.
- (b) While the likelihood and seriousness of potential privacy risks have been considered in the context of proposing mitigation strategies, this PIA does not provide an analysis at the level of detail set out in AS/NZS ISO 31000 (Risk management – Principles and Guidelines).
- (c) We have not undertaken any direct consultation with other external agencies, stakeholders or interest groups.

2.5 Qualifications and assumptions

This PIA report is subject to the following qualifications and assumptions:

- (a) any information not listed in Schedule 2 is not material to assessing the privacy impacts of the NOO Model; and
- (b) MinterEllison has not undertaken any consultation or investigations other than those set out in the Methodology at section 2.4.

2.6 Assessing community expectations

- (a) For the purposes of this PIA, our assumptions and conclusions about community expectations most likely to be held by persons whose privacy may be impacted by the NOO Model implementation are based on the Evaluation Report relating to the Opt-Out Trials.

2.7 Terminology

- (a) Unless indicated otherwise:
 - (i) references to an 'individual' or a 'healthcare recipient' means a natural person who receives, has received or may receive healthcare; and
 - (ii) terms used in this report which are defined in the MHR Act, have the same meaning as in the MHR Act.
- (b) Other terms and acronyms are defined in Schedule 3.
- (c) Pursuant to section 14(1)(b) of the MHR Act and regulation 2.1.1 of the *My Health Records Regulation 2012* (Cth) (**MHR Regulation**), the Agency is the 'System Operator' for the MHR system. However, in practice a number of the System Operator's functions and activities are undertaken by the following entities:
 - (i) the Chief Executive Medicare (delegated by the System Operator);
 - (ii) officers in the Department of Human Services (**DHS**) (sub-delegated by the Chief Executive Medicare); and
 - (iii) Accenture, contracted by the System Operator as the National Infrastructure Operator (**NIO**).
- (d) The Chief Executive Medicare and DHS officers also act in a number of different capacities in relation to the overall operation of the MHR system.

- 
- (e) For ease of reference and clarity, as well as consistency with the 2015 and 2016 PIAs, this report uses the following terms to differentiate between the entities who perform functions in relation to the MHR system:
- (i) **System Operator (DHS)** means the System Operator acting through DHS officers, who have been sub-delegated by the Chief Executive Medicare;
 - (ii) **System Operator (NIO)** means the System Operator acting through NIO as its contracted service provider;
 - (iii) **HI Service Operator** means the 'service operator' as defined in section 6 of the HI Act (i.e. the Chief Executive Medicare) acting through delegated officers of DHS;
 - (iv) **Medicare** means the Chief Executive Medicare, acting through delegated officers of DHS, and performing Medicare-related functions under the *National Health Act 1953* (Cth) (**National Health Act**) and the *Health Insurance Act 1973* (Cth) (**Health Insurance Act**); and
 - (v) **Chief Executive Medicare (Repository Operator)** means the Chief Executive Medicare, acting through delegated officers of DHS, and performing the functions of a registered repository operator under section 38 of the MHR Act.
- (f) As discussed further in section 6.4 of this report, the current arrangements relating to the performance of System Operator functions may change in the future. Unless indicated otherwise, references to the 'System Operator (DHS)' should also be read as including a third party service provider contracted by the Agency to perform functions and activities on behalf of the System Operator.

3. Description of NOO Model

3.1 Legislative authority

- (a) Clause 2 of Schedule 1 to the MHR Act provides for the Minister to make rules to apply the opt-out model³ nationally, but only if the Minister is satisfied that this would result in MHR system participation at a level that provides value for those using the MHR system.
- (b) We are instructed that based on the findings in the Evaluation Report, the Minister is satisfied that the implementation of an NOO Model would result in participation at a level that provides value for both individuals and healthcare providers. (It is outside the scope of this PIA to undertake a further assessment on this issue.)
- (c) A legislative instrument pursuant to clause 2 of Schedule 1 to the MHR Act is currently being drafted (**the NOO Rule**), and is proposed to be made by August 2017.
- (d) The MHR Act and HI Act contain provisions which authorise the collection, use and disclosure of health information, 'identifying information' (as defined under those Acts) and healthcare identifiers in certain circumstances by the System Operator, the HI Service Operator, the Chief Executive Medicare and other entities. A summary of these provisions is set out in section 2.4 of the 2016 PIA and therefore are not repeated in this report, other than to note that:
 - (i) section 72 of the MHR Act provides that an authorisation under that Act to collect, use and disclose health information is also an authorisation to collect, use or disclose the health information for the purposes of the Privacy Act;
 - (ii) section 73 of the MHR Act provides that a contravention of the MHR Act is an interference with privacy for the purposes of the Privacy Act;
 - (iii) section 28 of the HI Act provides that an authorisation under that Act to collect, use and disclose a healthcare identifier or identifying information is also an authorisation to collect, use or disclose that information for the purposes of the Privacy Act; and
 - (iv) section 29 of the HI Act provides that a contravention of the HI Act in connection with a healthcare recipient or individual healthcare provider is an interference with privacy for the purposes of the Privacy Act.

3.2 Implementation of NOO Model

- (a) The automatic creation of MHRs for individuals will be implemented through two streams:
 - (i) *Bulk registration*: All individuals who are eligible to participate in the bulk registration process (**'Eligible Bulk Registration (EBR) Individuals'**) at a point in time immediately before the commencement of the opt-out period will be automatically registered for a MHR unless they opt-out during the opt-out period. The eligibility criteria are set out in section 4.2 of this report. This will cover approximately 20 million individuals.
 - (ii) *Ongoing registration*: Individuals who enrol for Medicare or apply for an individual healthcare identifier (**IHI**) (e.g. newborns and immigrants) from a specified date will be given an opportunity to opt-out of MHR registration when they complete the Medicare enrolment or IHI application forms. If the individual does not opt-out, they will be registered for a MHR.

³ Part 2 of Schedule 1 to the MHR Act sets out the provisions relating to the opt-out model, including the circumstances in which the System Operator may register a health recipient for a MHR and eligibility for automatic registration.

- (b) The precise timing for the implementation of the bulk registration and ongoing registration processes have not been finally determined, as this will depend on factors such as the communications that will be undertaken by primary health networks (**PHNs**) and technological readiness. However, for the purposes of our assessment, we are instructed that the opt-out period for bulk registration:
 - (i) will commence no earlier than May 2018, and is proposed to end by December 2018 (however the NOO Rule will provide a flexible mechanism to prescribe the end date); and
 - (ii) will be for a minimum of three months.

3.3 Opt-out channels

Bulk registration

- (a) During the bulk Opt-Out Period (February – December 2018), an individual will be able to exercise their election not to be registered for a MHR via the following channels:
 - (i) an online opt-out service that will be hosted by the System Operator (DHS), but will be accessible via a link on the myhealthrecord.gov.au website (**MHR website**);⁴
 - (ii) a telephone help line operated by or on behalf of the System Operator (for example, via a DHS Customer Service Operator or third party contracted service provider); and
 - (iii) in person with the System Operator (for example, at a Service Centre operated by DHS or a third party contracted service provider).
- (b) Alternative channels will be made available to support 'hard to service' groups who are not able to reasonably access the above channels to exercise their right to opt-out. These groups include adult and juvenile prisoners, and defence force personnel deployed overseas.

Ongoing registration

- (c) Individuals will be able to notify the System Operator of their decision to opt-out when they apply to register with Medicare (including parents registering newborns or minors), or when they apply for an IHI.

Cancelling a MHR

- (d) Individuals will still be able to cancel their MHR at any time.
- (e) If a MHR already exists for an individual at the time that the individual seeks to opt-out (whether via the online, telephone or face-to-face channels), the individual will be advised that a MHR exists and given an opportunity to cancel their record in accordance with existing procedures.

3.4 Changes to information flows

- (a) This PIA focusses on the information flows and related privacy issues that are specific to the NOO Model implementation, and which are materially different to the information flows described in the 2015 and 2016 PIAs. The key variations are summarised as follows:
 - (i) In the Opt-Out Trials, the System Operator (DHS) transferred information about individuals to the System Operator (NIO) at the end of the opt-out period to create shell records. Under the proposed bulk registration process, this information will be provided ahead of the commencement of the opt-out period.

⁴ As at the date of writing, the MHR website is currently hosted by DOH but a transition to the Agency is being implemented.

- 
- (ii) There will be ongoing communication between the Service Provider (DHS) and the Service Provider (NIO) during the opt-out period in relation to the eligibility status of individuals for bulk registration, in particular whether an individual has opted-out of having a MHR automatically created for them.
 - (iii) There will not be a transition period following the end of the bulk registration opt-out period to allow individuals to set privacy controls for their MHR. If an individual wishes to set their privacy controls during the opt-out period, they will need to opt-in to have their MHR immediately created (rather than at the end of the opt-out period).
 - (iv) The communication approach relating to the opt-out process has been revised compared to the Opt-Out Trials. Individual letters will not be sent to people to advise them of the opt-out choice. Instead, the Agency will undertake public awareness raising activities, and funding will be provided to PHNs and consumer peak organisations to engage communications officers and implement communication strategies at the local level.
- (b) We understand that the process for ongoing registration will be substantively the same as the information flows outlined in the 2015 PIA (i.e. through the Medicare registration and IHI assignment processes).

4. Bulk registration & Opt-Out Process

4.1 Overview of bulk registration

- (a) Detailed information flows relating to the proposed bulk registration process using the Online Opt-Out Service are set out in Schedule 1. We understand that the information flows for the telephone and face-to-face channels will be substantially similar to the online process, except that a Service Centre or telephone helpline staff member will enter the relevant information into the system on behalf of the individual.
- (b) In summary:
 - (i) Ahead of the beginning of the opt-out period, a 'shell' record will be created for all EBR Individuals.
 - (ii) Individuals will have a (minimum) three month period to elect not to be automatically registered for a MHR via the online, telephone or face-to-face channels. An individual (e.g. a parent, guardian or authorised representative) will be able to opt-out a dependant or other person for whom they are the authorised representative, without having to opt-out themselves.
 - (iii) When an individual successfully opts-out of bulk registration, the shell record will be 'flagged'.
 - (iv) At the end of the opt-out period:
 - (A) flagged shell records (i.e. shell records for individuals who have opted-out of bulk registration) will be deleted;
 - (B) MHRs will be created for all EBR Individuals who have not opted out (i.e. individuals with non-flagged shell records), with the default privacy controls automatically applied;⁵ and
 - (C) individuals will be able to access their MHR and set privacy controls over both the content of, and access to, their MHR as well as notification settings.⁶
 - (v) However, a MHR will not be created for an individual if the System Operator considers that registration of the individual may compromise the security or integrity of the MHR system.⁷
 - (vi) If an individual wishes to set privacy controls and notification settings before the end of the opt-out period, they will need to 'create' their MHR by effectively opting in to MHR registration.
 - (vii) When either an individual or a healthcare provider accesses the individual's MHR for the first time, this will set off a 'trigger' to upload two years of retrospective Medicare-related data. This includes information (collectively referred to as **Medicare Data**) relating to prescriptions (from Pharmaceutical Benefits Scheme (**PBS**) or Repatriation Pharmaceutical Benefits Scheme (**RPBS**) data, healthcare provider visits (from Medicare Benefits Schedule (**MBS**) or Department of Veterans' Affairs (**DVA**) claims data, immunisations (from the Australian Immunisation Register (**AIR**), and organ donor status (from the Australian Organ Donor Register (**AODR**)).⁸

⁵ The default access and control settings are that all healthcare providers involved in the individual's care will be able to access, view all documents, and upload documents to the individual's MHR.

⁶ The existing privacy controls and notification settings will continue to be available. These are described in section 6.4.1 of the 2015 PIA.

⁷ MHR Act, Schedule 1, clause 3(1).

⁸ The Medicare Data flow process has been assessed in the 2015 PIA. Pursuant to clauses 12 and 13 of Schedule 1 in the MHR Act, the Chief Executive Medicare (Repository Operator) may provide health information to the System Operator for inclusion in an individual's MHR, unless the individual notifies the System Operator that they do not want to have this information included.

4.2 Identification of Eligible Bulk Registration Individuals

Eligibility for bulk registration participation

- (a) A person will be eligible to be included in the bulk opt-out registration where, immediately before the commencement of the opt-out period,⁹ they:
- (i) have a Medicare address situated in Australia (being the postal address held in the Medicare system for correspondence with the individual);¹⁰ and
 - (ii) have a verified IHI,
- unless they fall within one of the following eligibility exceptions:
- (iii) have an IHI record status of deceased, retired or resolved; or
 - (iv) have an IHI record flagged as being an intertwined record or possible duplicate record; or
 - (v) have a Medicare card or DVA health card end date recorded in the Medicare system; or
 - (vi) have a Medicare Individual Reference Number (**IRN**) of '0'; or
 - (vii) have an IHI that has a status of suppressed; or
 - (viii) have an active or suspended MHR; or
 - (ix) were a participant in the Opt-Out Trials and opted out.
- (b) EBR Individuals will be eligible to participate in the bulk opt-out registration regardless of whether they continue to reside at the same Australian Medicare address after that time.

Identification process

- (c) The System Operator (NIO) will request the System Operator (DHS) to provide the following information ("**HI Data Set**") for all EBR Individuals:
- (i) IHI number, IHI record status and IHI status;
 - (ii) first name and last name;
 - (iii) sex;
 - (iv) date of birth; and
 - (v) address (except for individuals under 18 years).
- The HI Data Set comprises an individual's healthcare identifier, as well as 'identifying information' within the meaning of section 9 of the MHR Act and section 7 of the HI Act.¹¹
- (d) The HI Service Operator will locate (use) and disclose to the System Operator (DHS) the HI Data Set of each individual that has an active verified IHI.
- (i) The use and disclosure of the HI Data Set of individuals (being information collected by the HI Service Operator for healthcare identifier assignment purposes) for the purpose of facilitating bulk MHR registration would be characterised as a secondary purpose in relation to APP 6. This will be permitted under APP 6.2(b), on the basis that the use and disclosure is authorised under section 15 of the HI Act.

⁹ The NOO Rules will either prescribe a date, or provide a mechanism by which a date will be specified.

¹⁰ This is consistent with the meaning of 'Medicare Address' in the *My Health Records (Opt-Out Trials) Rule 2016*, which is also proposed to be adopted in the new NOO Rule.

¹¹ See also regulation 5 of the *Healthcare Identifiers Regulations 2010* (Cth), and regulation 1.1.7 of the *My Health Records Regulation 2012* (Cth).

- 
- (ii) For the purposes of APP 3.1, the collection of the HI Data Set by the System Operator (DHS) is reasonably necessary for, and directly related to, the functions of the System Operator in relation to the implementation of the NOO Model. This is on the basis that the information is the minimum data required to identify EBR Individuals, and to create shell records and MHRs for those individuals. Further, the indirect collection of individual information will be permitted under APP 3.6(a)(ii), as the collection of healthcare identifiers and identifying information is authorised under item 1 of clause 8 of Schedule 1 to the MHR Act.
 - (e) Medicare will also locate (use) and disclose to the System Operator (DHS) a list of individuals who are not eligible for bulk registration because they have a Medicare address outside Australia, a Medicare or DVA end date, or a Medicare IRN of '0' recorded in the Medicare system. As at the date of writing, DHS and the Agency are currently developing business rules for determining eligibility for bulk registration, including the minimum data that will be required to match individuals between the Medicare database and the HI Service system. This will likely include information such as:
 - (i) 'identifying information' within the meaning of the MHR Act and HI Act, such as an individual's name, date of birth, Medicare card number and address, and
 - (ii) other personal information of an administrative nature, such as whether the individual's Medicare eligibility has ceased.
 - (f) The use and disclosure of the information sourced from the Medicare system (being information collected by Medicare for purposes relating to its functions under the Health Insurance Act and National Health Act) for bulk registration purposes will constitute a secondary purpose in relation to APP 6. This use and disclosure by Medicare will be permitted under APP 6.2(b), on the basis that the use and disclosure is authorised under the following legislative provisions:
 - (i) in relation to 'identifying information' - item 1 of clause 8 of Schedule 1 to the MHR Act; and
 - (ii) in relation to other Medicare information – subsection 130(1) of the Health Insurance Act.¹²
 - (g) For the purposes of APP 3.1, the collection of the information by the System Operator (DHS) is reasonably necessary for, and directly related to, the functions of the System Operator in relation to the implementation of the NOO Model. This is based on our understanding that the information provided by Medicare will be the minimum data required to identify non-EBR Individuals, so that shell records (and consequently MHRs) are not created for those individuals. The indirect collection of the information (insofar as it is 'identifying information') will be also permitted under APP 3.6(a)(ii), pursuant to the authorisation under item 1 of clause 8 of Schedule 1 to the MHR Act.
 - (h) The System Operator (DHS) will provide to the System Operator (NIO) the HI Data Sets relating to EBR Individuals, and the IHs of trial participants who opted-out of automatic MHR registration during the 2016 Opt-Out Trials.
 - (i) System filtering rules will remove information relating to non-EBR Individuals so that the System Operator (NIO) only receives HI Data Sets in relation to EBR Individuals. This is a privacy positive measure as it minimises risks relating to the unnecessary sharing of personal information, as well as reducing the risk of shell records being created for non-EBR Individuals.

¹² Subsection 130(1) of the Health Insurance Act allows the disclosure of information obtained under that Act, for the purposes of enabling a person to perform functions under the MHR Act (whether as a delegate or otherwise).

- (ii) For the purposes of APP 6, the provision of the above information by the System Operator (DHS) will constitute a 'use', on the basis that the NIO is a contracted service provider of the System Operator. The use of the information by both the System Operator (DHS) and the System Operator (NIO) will be in accordance with APP 6.1, as it will be provided and used for the primary purpose for which it was collected, that is, to ensure that shell records are only created for EBR Individuals.
- (iii) We understand that the list of trial participants who opted-out during the 2016 Opt-Out Trials will also be used by the System Operator (NIO) at the end of the opt-out period as a further check to ensure that, in the event that a shell record was created in error, MHRs will not be created.

Relevant recommendations in Previous Privacy Assessments

2016 Privacy Advice

- Recommendation 1 (DHS disclosure of information to the NIO for the NOO)
- Recommendation 2 (Maximum transparency about the bulk transfer process)

4.3 Communicating the opt-out choice and opt-out timing/approach

- (a) APP 5 requires an agency to take reasonable steps to notify an individual, or otherwise ensure that the individual is made aware, of certain matters relating to the collection of their personal information (as specified in APP 5.2). More rigorous steps are likely to be required where 'sensitive information' such as health information will be collected.¹³
- (b) As noted in the 2015 and 2016 PIAs, a key privacy issue in relation to implementing an opt-out model is ensuring individuals are given sufficient information to make informed choices about MHRs, including opting-out and adjusting privacy control settings (and how to exercise those choices).
- (c) Effective communication is important not only from an APP 5 compliance perspective, but also in relation to meeting community expectations and increasing public confidence in the MHR system. This is reflected in the findings of the Opt-Out Trials evaluation where, after being provided with an explanation of the MHR system and its benefits and what automatic registration meant, the majority of survey and focus group participants indicated that they had more positive feelings about the automatic creation of a MHR, and their concerns about privacy and security were either low or had disappeared.¹⁴
- (d) The challenge with a bulk registration process is reaching approximately 20 million individuals to ensure they are given a reasonable opportunity to exercise their right to opt-out of bulk registration. Failure to adequately notify or make individuals aware of the bulk registration and its implications could lead to public concerns about the handling of their health information, particularly as MHRs will become available to registered healthcare provider organisations once created (unless the individual has set up their MHR privacy controls).

Proposed communication strategy

- (e) For the Opt-Out Trials, a letter and brochure was sent to each trial participant before the beginning of the opt-out period. However, this will not occur for the NOO bulk registration process. The decision not to send personalised letters has been informed by the Evaluation Report which found that this strategy had not been effective in creating awareness and understanding of the MHR system. In particular, feedback from surveys and focus groups indicated that:

¹³ APP Guidelines, paragraph 5.4.

¹⁴ Evaluation Report, Executive Summary, pages vi and xii.

- 
- (i) a majority of people either did not recall receiving the letter, or discarded the letter and brochure as 'junk mail'; and
 - (ii) for those that did read the letter and brochure, few understood the content, or they did not act on it as the letter implied that they would receive a follow up communication or otherwise gave 'mixed messages'.¹⁵
- (f) We are instructed that while the communication strategy for the bulk registration process is still being developed, it will include the following activities at the national and local level:
- (i) Funding will be provided to PHNs and consumer peak organisations to determine the most effective forms of communication in their local communities. In particular, PHNs will develop and implement communication strategies to reach vulnerable and disadvantaged individuals, such as people from culturally and linguistically diverse backgrounds, indigenous people, homeless persons, and adults with limited or no capacity.
 - (ii) The Agency is currently consulting with PHNs, consumer peak groups and other consumer organisations in relation to the development of central materials (e.g. fact sheets) for both the general community as well as vulnerable and disadvantaged groups. These materials may be tailored by PHNs for the local audience.
 - (iii) DOH is working with relevant State and Territory government agencies to facilitate opt-out arrangements for adult and juvenile prisoners, and defence personnel deployed overseas, including the development of appropriate communication strategies to target these hard to service groups.
 - (iv) There will be public relations and community engagement events, including supporting 'local champions' from consumer groups, the health sector and the medical profession to explain the benefits of the MHR system. There will also be a social medial campaign.
 - (v) We understand that at this time, a national television, newspaper and radio awareness campaign is not proposed. It will be a matter for PHNs to decide whether to develop and run these at the local level.
- (g) A risk that arises with the proposed bulk registration process is the potential for individuals to claim that they were unaware of the fact that a MHR would be automatically created unless they took action to opt-out. Individuals will not receive direct notification of the bulk registration, or written confirmation when a MHR has been created for them. If communications relating to the NOO Model implementation do not reach an individual (or those communications are not clearly understood), an individual's MHR could potentially exist for years without their knowledge, during which time healthcare providers could be accessing the individual's MHR and viewing their health information (including retrospective Medicare Data.)
- (h) In order to reach all segments of the community, communications about the opt-out process should be 'everywhere' and available in multiple formats and channels and both the national and local levels.¹⁶
- (i) We also note that there will need to be adequate resourcing for the telephone and face-to-face channels to answer inquiries about the MHR system and opt-out process.

¹⁵ Evaluation Report, pages ii, viii, xix, 54, 83-84, 91-92.

¹⁶ Evaluation Report, page 42.

Recommendation 1: Ensure that consistent communications relating to the bulk registration and opt-out process, which may be delivered through a range of activities and media channels, reach as much of the Australian community as possible.

The communication activities should continue following the end of the opt-out period to alert individuals to the fact (in case they were not alerted during the opt-out period) that:

- unless they opted out, they will now have a MHR;
- the individual can set privacy controls to restrict who can see, and what information is included in, their MHR;
- the individual can cancel their MHR if they do not want it.

Recommendation 2: Sufficient resources should be made available in Service Centres and the MHR helpline call centre for dealing with inquiries relating to the bulk registration and opt-out processes in the lead up, during and following the opt-out period. This may include:

- the allocation of adequate staffing levels to deal with inquires in a timely manner, particularly during periods and times of peak demand; and
- accessible information to support staff in responding to inquiries quickly and in a consistent manner (e.g. 'Frequently Asked Questions' and other written materials).

Phased approach

- (j) A phased approach to bulk registration is being considered whereby the opt-out period and MHR creation may be staggered, most likely on a jurisdictional basis.
- (k) Potential risks with a phased approach include:
 - (i) the risk of causing confusion amongst individuals as to when they can opt-out; and
 - (ii) if an individual moves interstate before or during the opt-out period, there is a risk that they may miss out on the opportunity to opt-out (noting that individuals may not necessarily keep their Medicare address details up-to-date, making it difficult to identify who these affected individuals may be).

Recommendation 3: A single bulk registration implementation process (as opposed to a phased approach) would be preferable in terms of minimising confusion and the risk of certain individuals (such as those who may have moved, or be in the process of moving, interstate) inadvertently missing out on the opportunity to opt-out.

However, if a phased approach is adopted, the communication strategy and content should include the provision of accessible information to the public about the timeframes for each phase (i.e. the period during which individuals living in certain jurisdictions can opt-out).

4.4 Limits to choice of opt-out channel

- (a) EBR Individuals aged 14 years and over will generally be able to opt-out of the MHR system via the online, telephone and face-to-face opt-out channels.
- (b) However, only the face-to-face channel will be available to the following individuals:
 - (i) individuals under the age of 14 years who are able to demonstrate their capacity and satisfy the current requirements of independent minors;
 - (ii) an individual (the first individual) who wishes to opt-out another individual (the second individual) who is:
 - (A) under 18 years and not listed on the first individual's Medicare card; or

- (B) a person over 18 years who lacks capacity to make decisions for themselves.
- (c) There may be practical difficulties in enabling the above types of individuals to exercise the right to opt-out where they are unable to attend a Service Centre, for example where the person is in a remote area that does not have a local Service Centre, or where they are unable to travel to a Service Centre due to disability, illness or other reason.
- (d) We note that this issue was also considered in the 2016 PIA in the context of the Opt-Out Trials.

Recommendation 4: To ensure certain individuals who live in remote areas or are otherwise unable to travel to a Service Centre are able to exercise the opt-out choice, further consideration should be given to providing alternative means to opt-out. This could include, for example:

- making available alternative face-to-face channel mechanisms (e.g. online/video conferencing) or venues; and/or
- allowing a telephone channel to be used, subject to the provision of relevant supporting evidence (by post or email) within a specified period.

Relevant recommendations in Previous Privacy Assessments

2016 PIA

- Recommendation 3 (Alternative opt-out channels for individuals in remote areas)

4.5 Pseudonymous records and registration

- (a) APP 2 requires agencies to give individuals the option of interacting with the agency on an anonymous or pseudonymous basis, unless it would be impracticable to do so, or where dealing with an identified individual is authorised or required by law.
- (b) Under the current MHR system, individuals may hold a pseudonymous MHR if they hold a pseudonymous IHI.
- (c) As part of the bulk registration, there may be individuals who have a non-pseudonymous IHI, but who may wish to have a pseudonymous MHR. We understand that:
 - (i) an individual can have a pseudonymous and non-pseudonymous MHR;
 - (ii) if an individual only wants a pseudonymous MHR, they will need to first opt-out of bulk registration, then (in accordance with existing processes) apply to the HI Service Operator for a pseudonymous IHI,¹⁷ and subsequently apply to the System Operator (DHS) for a pseudonymous MHR (i.e. effectively opting back in, but on a pseudonymous basis); and
 - (iii) the proposed communication strategy will include providing the public with information about the option of obtaining a pseudonymous MHR, and how they can obtain this (including information on the MHR website).

¹⁷ An individual can apply for a pseudonymous IHI by completing the form available at <https://www.humanservices.gov.au/customer/forms/ms005>.

- 
- (d) Individuals who hold a pseudonymous IHI at the beginning of the opt-in period will not be identified as EBR Individuals. This is because pseudonymous IHIs are not linked to a Medicare address, and an individual must have a verified IHI and Medicare address situated in Australia to be eligible for bulk registration participation. This process will mitigate the risk of duplicate MHRs being automatically created at the end of the opt-out period for individuals who already have a pseudonymous IHI, as well as ensuring that MHRs are not created for those people who do not want a record.
 - (e) There may be some individuals with pseudonymous IHIs who do not have a MHR but want one. We understand that these individuals will need to apply for a pseudonymous MHR in accordance with existing processes (effectively opting in for registration).
 - (f) We also understand that the Agency is currently liaising with DHS (as the HI Service Operator) to develop a communication strategy to target holders of pseudonymous IHIs and inform them about the bulk registration and opt-out process.

Recommendation 5: The communication strategy targeting individuals who currently hold a pseudonymous IHI should provide individuals with information (or tell them where they can find information) about:

- what they need to do if they do not have a MHR but would like to have one created;
- what they need to do (if anything) if they have a MHR.

4.6 Reasons for opting-out

- (a) In each of the opt-out channels, individuals will be asked to provide a reason as to why they have chosen to opt-out themselves or another person. The reason can be selected from one of following six choices, and will be voluntary.
 - (i) *'I have no use for a digital health record';*
 - (ii) *'I prefer to manage my health records on my own';*
 - (iii) *'I prefer that my doctor manages my health records';*
 - (iv) *'I am concerned about others having access to my private medical information';*
 - (v) *'I am concerned about the security of my medical information stored online';*
 - (vi) *'I do not trust what the Government or others will do with my medical information'.*
- (b) We understand that the System Operator will collect and use an individual's reasons for opting out for evaluation, analysis and reporting purposes. For example, this information may assist the System Operator to identify public concerns about the MHR system, and inform the development of improvements to the MHR system (e.g. privacy controls) and communications relating to the system. These purposes are consistent with the System Operator's functions under the MHR Act, and therefore the collection of opt-out reasons would be in accordance with APP 3.1.
- (c) APP 3.6 will also be satisfied on the basis that the opt-out reason will either be collected directly from the individual or their authorised representative.
- (d) To enable individuals to make an informed choice as to whether they provide opt-out reasons, and to promote compliance with APP 5 collection notice requirements, individuals should be made aware of the purpose of collection, and the fact that the provision of the information is voluntary.
- (e) Further, the purposes for which opt-out reasons will be used by the System Operator may be able to be achieved through the use of de-identified information. This would assist in reducing potential data security risks relating to the retention of identifiable information.

Recommendation 6: The design of the Online Opt-Out Service channel should make it clear that an individual's reason for opting out is an optional field. Information should also be made available (whether through the MHR website or privacy policy, or the Online Opt-Out Service itself) about the purposes for which the opt-out reasons will be used by the System Operator.

In relation to the telephone and face-to-face channels, scripts for Service Centre and MHR helpline staff should also address these matters.

Recommendation 7: Consideration should be given as to whether opt-out reasons provided by an individual could be collected and retained in a de-identified form. Aside from reducing any potential risks relating to data security or other misuse, this may also address any potential privacy concerns individuals may have about providing this information.

4.7 Setting privacy controls

- (a) The current privacy controls available under the opt-in model will continue to be available under the NOO Model.
- (b) It is proposed that:
 - (i) individuals will be able to set privacy controls to their MHR at the end of the opt-out period when their record has been created; and
 - (ii) if an individual wishes to choose to set their privacy controls during the opt-out period, they will need to opt-in to have their MHR created in accordance with existing arrangements. The individual's record will then become immediately available to healthcare provider organisations, subject to any privacy controls set by the individual.
- (c) Privacy controls will not be able to be set through the Online Opt-Out Service or the MHR website. An individual will need to set up a myGov account and then link their MHR in order to access it.
- (d) We note that the majority of consumers who were consulted by Deloitte in relation to the recommendations made in the 2013 review of the MHR system indicated that they were unlikely to set privacy controls to block access to their MHR, or to particular documents in their MHR, *'except in very special circumstances'*.¹⁸ The Evaluation Report relating to the Opt-Out Trials also found that the rate of Opt-Out Trial participants who restricted access to their MHR was low (less than 0.5%).¹⁹
- (e) The possibility of allowing a transition period to set access controls following the end of the opt-out period (whereby an individual could set their preferred access and content control settings before their MHR became available for health providers to access) was considered by the Agency as part of the Opt-Out Trials. This proposal was ultimately rejected as the potential privacy benefits in providing such a transition period were considered to be outweighed by:
 - (i) the complexity of effectively communicating the relevant timeframes for opting-out and setting privacy controls;
 - (ii) the risk of creating confusion around the opt-out period and when an individual's MHR would become available to healthcare providers; and
 - (iii) the likelihood that an individual will apply privacy controls if they have context for what information will be included in their MHR.

¹⁸ Deloitte report, page 2.

¹⁹ Evaluation Report, page 31.



- (f) In the context of the proposed bulk registration process, the potential risk is that some individuals may claim that they did not understand when their MHR would be created and become available to healthcare providers, and when and how to set their privacy controls. This risk may be mitigated by:
- (i) ensuring that there is an effective communication strategy during, and following, the opt-out period to clearly inform individuals about the consequences (and timeframes) for opting-out, and the fact that they can set privacy controls in relation to their MHR (see **Recommendations 1 and 3**); and
 - (ii) the fact that individuals will be able to view who has accessed their MHR and uploaded documents.
- (g) The Evaluation Report relating to the Opt-Out Trials identified difficulties in accessing MHRs through myGov as presenting a barrier to participation and use of the MHR system by individuals.²⁰ These difficulties may also present barriers in relation to allowing an individual to set their privacy control and notification settings. The potential consequence of this is that a MHR may be accessed by a healthcare provider (which will trigger the Medicare Data flow) before the individual has been able to create a myGov account.

Recommendation 8: As part of the opt-out communications (and, if possible, where an individual attempts to set their MHR privacy controls during the opt-out period), information should be provided to individuals about the effect of setting privacy controls, that is, that their MHR will become immediately available for health providers to access, subject to the individual's set privacy controls.

Relevant recommendations in Previous Privacy Assessments

2015 PIA

- Recommendation 29 (Allowing some privacy settings to be adjusted via the Online Opt-Out Service)
- Recommendation 32 (Standalone MHR individual access portal separate to myGov)

²⁰ Evaluation Report, pages xi and xv.

5. Ongoing opt-out registration

5.1 Overview of ongoing registration arrangements

- (a) From a specified date (currently proposed to align with the bulk registration process), any individual who is registered for Medicare or an IHI, will be automatically registered for a MHR unless they opt-out. This includes:
 - (i) newborn children; and
 - (ii) immigrants to Australia.
- (b) An individual will be able to choose not to be registered for a MHR (or a parent/guardian in relation to a newborn child) when completing an application to enrol in Medicare (including for newborns) or registering for an IHI. An individual will be able to opt-out another person without having to opt-out themselves, and will be able to opt-out themselves without having to opt-out another person. For example, a parent will be able to opt-out their child without impacting their own MHR.
- (c) The forms currently used by Medicare and the HI Service Operator to enable individuals to apply for Medicare enrolment and registration in the HI Service will be updated to provide an option for individuals to notify the System Operator of their opt-out decision (for example, a check box or other mechanism). If an application provides for the entry of multiple individuals, an opt-out option will be available in respect of each person.
- (d) We understand that at the time they register with Medicare or apply to create an IHI, these individuals will not have a verified IHI. However, the successful processing of the application will result in a verified IHI, at which point the System Operator will recognise them as eligible for MHR registration. The System Operator would then immediately create a MHR for the individual, unless the individual has opted out and subject to the System Operator's discretion not to register particular individual (for example, where the System Operator considers the registration would compromise the security and integrity of the MHR system).

5.2 Consideration of privacy issues

- (a) The proposed ongoing registration arrangements for the NOO Model implementation is consistent with the proposed process for 'Automatic registration of new Medicare enrolments and IHI registrants' that was assessed in the 2015 PIA. We note that in the 2015 PIA, the possibility of allowing a transition period to set privacy controls in relation to ongoing registration (whereby access to an individual's MHR would be suspended for a period during which an individual or authorised representative could set their preferred access and content control settings) was considered but ultimately rejected. This was because the potential privacy impacts were mitigated by the fact that individuals registering for Medicare or applying for an IHI for the first time:
 - (i) will not have any historical Medicare data; and
 - (ii) will be given the opt-out choice when they proactively apply for Medicare enrolment or IHI assignment.
- (b) There is a possibility that following the commencement of the ongoing registration arrangements, individuals may complete forms which do not have the opt-out choice (for example, where a hospital provides the parent of a newborn child with the current 'opt-in' Medicare enrolment form).
- (c) It will also be important to ensure that individuals who apply for an IHI through DVA are provided with an opportunity to opt-out.



Recommendation 9: For the purposes of the ongoing registration arrangements, processes and system business rules should be implemented to ensure that a person is not automatically registered for a MHR where they have completed an (old) application form for Medicare enrolment or IHI assignment that is based on the opt-in model.

In these circumstances, the individual or their authorised representative should receive a confirmation that they have not been registered for a MHR, and be provided with information as to how they can apply for a MHR. This could be provided, for example, as part of the confirmation of Medicare enrolment or IHI assignment.

Relevant recommendations in Previous Privacy Assessments

2015 PIA

- Recommendations 25 and 26 (Information for inclusion in Newborn Child Declaration)
- Recommendation 27 (Information for inclusion in application forms for Medicare enrolment and IHI assignment)
- Recommendation 28 (Providing individuals who will be issued an IHI through DVA the opportunity to opt-out of automatic MHR registration)

6. Other privacy issues

6.1 Data quality

- (a) APP 10 requires agencies to take reasonable steps to ensure that the personal information collected, used and disclosed by the MHR system is accurate, up-to-date and complete, and relevant for the purpose of its use and disclosure.
- (b) Incorrect clinical data can have adverse consequences for individuals, including negative health outcomes resulting from clinical decision-making errors (based on incorrect data), as well as embarrassment or emotional distress. As the number of individuals with MHRs substantially increases under an NOO Model, so too does the potential for data quality risks.
- (c) We understand that the Opt-Out Trials did not include any auditing or testing in relation to data accuracy issues relating to automatic registration, the creation of shell records or Medicare data flows.
- (d) Privacy issues relating to data quality in an NOO Model have been considered in the 2015 PIA and the 2016 Privacy Advice, and the discussion set out in those previous privacy assessments will not be repeated here.
- (e) We note that:
 - (i) healthcare providers are subject to existing professional and clinical standards relating to patient health records, which apply to information that is uploaded to an individual's MHR; and
 - (ii) under rule 29 of the *My Health Records Rule 2016 (MHR Rule)*, healthcare provider organisations are required to take reasonable steps to ensure that the organisation and their employees exercise due care and skill so that any record uploaded to the MHR system *'is, at the time the record is uploaded, accurate, up-to-date, not misleading and not defamatory'*.
- (f) These obligations on healthcare providers assist in mitigating potential data quality risks.
- (g) The MHR website also contains information about what steps an individual can take if they think the content of their MHR is incorrect, and a help line is available for individuals to report issues which will be investigated by the System Operator.²¹
- (h) Further, if the System Operator becomes aware of an issue relating to the accuracy or quality of information included in an individual's MHR (for example, in response to an enquiry or complaint made by an individual), section 73B of the MHR Act allows the System Operator to:
 - (i) request the relevant healthcare provider organisation to correct the information and upload the corrected record to the MHR system; and
 - (ii) if the provider refuses to do so - issue a direction (with which the provider is required under the MHR Act to comply) that the provider attach a note prepared by the individual healthcare recipient to the record, and to upload the record and note to the MHR system.
- (i) This power, when exercised, assists the System Operator to meet its obligations under both APP 10 and APP 13 (correction of personal information).

²¹ <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/find-out-more?OpenDocument&cat=Managing%20your%20My%20Health%20Record> (accessed May 2017).

- (j) The only information not covered by the Previous Privacy Assessments in relation to data quality is that the System Operator will be collecting and using information about an individual's reason for opting out of bulk registration. As discussed earlier in this report, this information will be collected directly from the individual or their authorised representative (via the online, telephone or face-to-face channels) at a point in time when the individual opts-out, and will be voluntarily provided based on a choice of six specified reasons. Having regard to the nature of the information and the purpose for which it will be collected and used, we consider APP 10 will be satisfied.
- (k) We do not propose to make any recommendations in relation to APP 10 further to those set out in the 2015 PIA and 2016 Privacy Advice.

Relevant recommendations in Previous Privacy Assessments

2015 PIA

- Recommendation 34 (Opt-out website links to existing clinical safety audits)
- Recommendation 35 (Updated review of data quality risks posed by the use of IHIs and Medicare provided data)

2016 Privacy Advice

- Recommendation 4 (My Health Record data quality)

6.2 Data security

- (a) APP 11 requires agencies to take reasonable steps to protect the personal information it holds from misuse interference and loss, and from unauthorised access, modification or disclosure.
- (b) Under section 17 of the MHR Act, the System Operator is required to retain a record relating to a healthcare recipient which has been uploaded to the National Repositories Service, until 30 years after the death of the healthcare recipient or, if the System Operator does not know the date of death, until 130 years after the health recipient's date of birth. These obligations continue to apply even after an individual cancels their MHR registration. (In this circumstance, we understand that the record will be deactivated, and can later be reactivated if the individual decides to opt back in.)
- (c) The implementation of the NOO Model is expected to result in an increase in the number of MHRs from under 5 million to more than 23 million. The significant increase in the number of individuals, together with the richness of the information and the extended MHR data retention periods, will also increase the likelihood and severity of security risks to the MHR system.
- (d) We are instructed that the MHR system has been designed in anticipation of an NOO Model. It is beyond the scope of this PIA to assess security arrangements for the MHR system under an NOO Model, as this requires expert technical assessment. We also note that a number of likely data security risks were considered in the 2015 PIA. However, it is critical that such an assessment be undertaken before the NOO implementation commences. In particular, while we understand that the MHR system has been resilient to date against external attacks (for example, the WannaCry ransomware in May 2017), cyber security threats present a significant ongoing risk to the MHR system, both in relation to the exposure of MHRs, as well as preventing access by individuals and their healthcare providers to MHRs.

Recommendation 10: Before the NOO implementation commences, the Agency should commission (or review and update any existing) information security Threat and Risk Assessment in relation to the MHR system. The scope of the assessment should include consideration of:

- the bulk registration process, including in particular the transfer of data about individuals to the System Operator (NIO) and the creation of shell records at the beginning of the opt-out period, before individuals are given an opportunity to opt-out;
- cyber security threats; and
- any security risk assessments undertaken by DHS and/or the Digital Transformation Agency in relation to myGov, and how any identified risks may impact on an individual's ability to access their MHR (having regard to the increase in MHR system users under an opt-out model).

Relevant recommendations in Previous Privacy Assessments

2015 PIA

- Recommendation 37 (Threat and Risk Assessment)
- Recommendation 40 (De-identification Protocol)

6.3 Complaints and incident management

- (a) APP 1.2 requires the Agency, as the System Operator, to implement practices, procedures and systems to enable it to deal with inquiries or complaints about its compliance with the APPs. It is also a function of the System Operator under section 15(j) of the MHR Act to establish a complaints handling mechanism in relation to the MHR system.
- (b) The implementation of incident management systems and procedures is consistent with the System Operator's data security obligations under APP 10. Further, complaints and incident management procedures assist the System Operator to comply with its data breach notification obligations under section 75 of the MHR Act.
- (c) Between 1 July 2012 to 30 June 2017 (the first five years of the operation of the MHR system), a total of 330 complaints were received by the System Operator. The majority of these complaints were made by individuals (94%) and were received by telephone (80%).²² The top five issues raised were:
 - (i) technical issues relating to the myGov website (22%);
 - (ii) assisted registration issues, including concerns with consent and provision of the Identity Verification Code (14%);
 - (iii) privacy concerns (e.g. where an individual believed they were registered for a MHR without their consent) (10%);
 - (iv) dissatisfaction with the design or operation of the MHR system (10%); and
 - (v) dissatisfaction with communication (e.g. long waiting periods on the helpline, receiving multiple letters, etc) (10%).

²² Statistics on MHR privacy complaints and privacy breaches, provided by the Agency on 20 June 2017.

- 
- (d) These figures suggest that there have been relatively few privacy complaints during the first few years of the MHR system's operation under the opt-in model. However, the move to the NOO Model is likely to lead to an increase in both the number and proportion of complaints, for example individuals who may claim that they were not aware a MHR would be created for them unless they opted out (and potentially may not become aware until years after its creation). An effective communication strategy will play an important role in mitigating the extent of this risk (see **Recommendation 1**).
 - (e) Further, as the size and complexity of the MHR system grows, with an ever increasing use of the system by both individuals and healthcare providers, the likelihood of an increase in the number of incidents of non-compliance with the My Health Record legislation, privacy breaches and even fraud is a reality.²³
 - (f) Issues relating to the management of privacy complains and incidents were considered as part of the 2015 PIA. For the purposes of this PIA, we have been asked to consider the scalability of the current complaints and incident management processes in relation to the NOO Model.

Current complaints management process

- (g) The System Operator's complaints management procedures are set out in a document called the *My Health Record—Complaints Handling Process (Complaint Handling Process)*. We understand that the Complaint Handling Process is under review by the Agency, but remains current as at the time of this PIA.
- (h) The Complaints Handling Process provides guidance for staff within both the Agency and DHS who are *'involved in the management and resolution of complaints related to the My Health Record system'*.²⁴ It covers complaints relating to any expression of dissatisfaction made in relation to the MHR system itself, the delivery of associated services (e.g. registrations, decisions made by the System Operator, document uploads) and the conduct of individuals who deliver those services (e.g. registration staff, the System Operator, healthcare providers, repository operators, eHealth helpline staff).²⁵
- (i) Complaints may be made in by post, by telephone or in person at a Service Centre. Each of these complaints channels is managed by DHS.
- (j) The Complaints Handling Process applies a tiered management approach based on the nature or complexity of the issue. In brief summary:
 - (i) A complaint is initially received by DHS, and is recorded by a DHS staff member in DHS's Customer Relationship Management (**CRM**) system.
 - (ii) The Compliance Section (staffed by DHS officers) monitors the CRM daily to identify new complaints recorded in CRM. The Compliance Section will also receive notification of a new complaint by way of email from the CRM. On identification/receipt of a new complaint, the Compliance Section records relevant details about the complaint in an Excel spreadsheet (**complaints database**).
 - (iii) Complaints about privacy or clinical safety matters are managed by the Compliance Section. Other types of complaints are referred to the relevant internal area best placed to respond to the issues raised in the complaint. The Compliance Section maintains visibility on the progress of all complaints that are escalated by DHS, and is responsible for contacting stakeholders as required.
 - (iv) DHS will escalate a complaint to the Agency (as the System Operator) if it cannot be resolved internally by DHS, or has been identified under agreed protocols as one for mandatory escalation.

²³ Since the operation of the MHR system commenced, there have been 10 privacy breaches reported by the System Operator to the OAIC, affecting a total of 77 consumers (statistics provided by the Agency on 20 June 2017).

²⁴ *My Health Record—Complaints Handling Process*, page 5.

²⁵ *My Health Record—Complaints Handling Process*, page 6.

Current incident management process

- (k) The System Operator's complaints management procedures are set out in a document called the *Compliance Procedures—Compliance Incident Management Procedures (Incident Management Procedures)*, and form part of the broader My Health Record Incident Management Framework (IMF). The Incident Management Process is presently under review by the Agency, but remains current as at the time of this PIA.
- (l) The scope of the Incident Management Procedures relates to incidents that constitute '*an unplanned interruption or reduction in the quality of the My Health Record System and associated systems and services, which may or may not have an impact on consumer care*'.
- (m) The Incident Management Procedures currently tasks six positions with responsibility for coordinating incident responses. While this may be sufficient for present purposes, increased resourcing will be required in proportion to an increase in the volume and complexity of incidents.

Scalability of the current complaints and incident management procedures

- (n) Given the likelihood of a material increase in the number of potential complaints and incidents (commensurate with the increase in the number of individuals with MHRs), there is a need to ensure that channels for making complaints are sufficiently resourced to handle the volume of inquiries, and that staff receiving those complaints are sufficiently trained to answer questions and to accurately record interactions in the relevant systems.
- (o) There is also a need to ensure sufficient resourcing of both the incident management team and the complaints handling team, who are responsible for handling the incident or complaint after receipt.
- (p) Sufficient resourcing of both the front end and back end of incident and complaint management will assist in promoting and maintaining the confidence of stakeholders in the system. This will be particularly important during and following the bulk registration opt-out period when large volumes of people may have inquiries or complaints about the opt-out process or setting MHR privacy controls.²⁶
- (q) Further, while the Incident Management Procedures and the Complaints Handling Processes are comprehensive, they do not (and cannot) provide complete guidance to staff investigating incidents and complaints. Having regard to the likely increase in the number of staff using the incident and complaint handling processes, and the increase in volume and complexity of incidents and complaints, it will be important to ensure that issues are resolved as efficiently and consistently and possible. Potential options to assist in achieving this may include:
 - (i) implementing central contact points for staff investigating incidents and complaints respectively, to obtain clarification on any matters; or
 - (ii) allocating dedicated incident managers or 'subject matter experts' according to incident types.
- (r) The use of an Excel spreadsheet as the complaints database creates potential risks in relation to the integrity of accurately recording a complaint, and may not be an effective means of managing and reporting on complaints as the number of individuals and participants in the MHR system (and consequently, the number of potential complaints) increases. In particular:
 - (i) it involves the manual duplication of a complaint from one database (CRM) to another (the spreadsheet), which creates a risk of inconsistency between the two databases. This risk is increased given that the input fields in the complaints database differ from those used in the CRM;

²⁶ Evaluation Report, page 195. This is reflected in the feedback received from stakeholders following the Opt-Out Trials. Stakeholders emphasised the need to ensure that the helplines for both individuals and healthcare providers were equipped and capable to handle the volume and nature of enquiries.

- (ii) there is a risk that an amendment to a complaint in one of the databases (after initially recorded) will not be reflected in the other database, leading to potential inconsistencies which could impact upon timely complaints resolution;
- (iii) the two methods by which the Compliance Section become aware of a complaint creates is a risk that complaints could be duplicated in the complaints database; and
- (iv) given the likely increase in the volume of complaints, an Excel spreadsheet is likely to become unworkable with the number of DHS staff requiring access to the document.

Recommendation 11: As part of the review of the complaints and incident management procedures, consideration should be given to:

- implementing appropriate systems which support accurate and consistent recording, tracking and reporting of large volumes of privacy and data security complaints and incidents; and
- ensuring an appropriate governance and management structure is in place, and that sufficient resources are allocated.

Relevant recommendations in Previous Privacy Assessments

2016 Privacy Advice

- Recommendation 5 (Seamless and well-resourced enquires and complaints processes)

6.4 Changes to opt-out service arrangements

- (a) While the Agency is the System Operator of the MHR system (as defined under the MHR Act), in practice a number of the System Operator's functions and activities are performed and delivered by DHS and its officers. This occurs by way of delegation by the System Operator to the Chief Executive Medicare under section 98 of the MHR Act, and sub-delegations by the Chief Executive Medicare to DHS officers.
- (b) However, the current arrangements relating to the performance of functions and activities relating to the MHR system could change in the future.
- (c) If certain System Operator functions or activities were to be outsourced to a contracted service provider:
 - (i) the contracted service provider and its employees would be authorised to handle personal information in the same manner as the System Operator under the MHR Act;²⁷
 - (ii) the contracted service provider must not be allowed to hold, transfer or handle records relating to the to the MHR system outside of Australia;
 - (iii) transition arrangements would need to be implemented to ensure the seamless delivery of services to individuals and healthcare providers, including the transfer of relevant records; and
 - (iv) existing processes and procedures relating to the management of the My Health Record would need to be reviewed and updated to reflect the changed service delivery arrangements, for example complaints and incident management procedures and data exchange processes.

²⁷ MHR Act, section 99.



Relevant recommendations in Previous Privacy Assessments

2016 Privacy Advice

- Recommendation 6 (Risk assessment and due diligence before making decision to outsource the Opt-Out Service)



7. Conclusions

7.1 Privacy positives

- (a) There are a number of existing privacy controls built into the MHR system which will remain under the NOO Model, which are identified at section 9.1.1 of the 2015 PIA.
- (b) The following additional privacy controls are proposed as part of the NOO implementation:
 - (i) each EBR Individual can opt-out of automatic bulk registration, which prevents a MHR from being created;
 - (ii) shell records will not include any Medicare Data or clinical content; and
 - (iii) live feeds will be sent from the opt-out service system to flag shell records relating to individuals who have opted out, and those shell records will be subsequently deleted, so that MHR records are not created for those individuals.

7.2 Privacy risks and recommendations

- (a) Our recommendations to mitigate privacy risks identified in this report are set out in full below.

Recommendation 1: Ensure that consistent communications relating to the bulk registration and opt-out process, which may be delivered through a range of communication activities and media channels, reach as much of the Australian community as possible.

The communication activities should continue following the end of the opt-out period to alert individuals to the fact (in case they were not alerted during the opt-out period) that:

- unless they opted out, they will now have a MHR;
- the individual can set privacy controls to restrict who can see, and what information is included in, their MHR;
- the individual can cancel their MHR if they do not want it.

Recommendation 2: Sufficient resources should be made available in Service Centres and the MHR helpline call centre for dealing with inquiries relating to the bulk registration and opt-out processes in the lead up, during and following the opt-out period. This may include:

- the allocation of adequate staffing levels to deal with inquires in a timely manner, particularly during periods and times of peak demand; and
- accessible information to support staff in responding to inquires quickly and in a consistent manner (e.g. 'Frequently Asked Questions' and other written materials).

Recommendation 3: A single bulk registration implementation process (as opposed to a phased approach) would be preferable in terms of minimising confusion and the risk of certain individuals (such as those who may have moved, or be in the process of moving, interstate) inadvertently missing out on the opportunity to opt-out.

However, if a phased approach is adopted, the communication strategy and content should include the provision of accessible information to the public about the timeframes for each phase (i.e. the period during which individuals living in certain jurisdictions can opt-out).



Recommendation 4: To ensure certain individuals who live in remote areas or are otherwise unable to travel to a Service Centre are able to exercise the opt-out choice, further consideration should be given to providing alternative means to opt-out. This could include, for example:

- making available alternative face-to-face channel mechanisms (e.g. online/video conferencing) or venues; and/or
- allowing a telephone channel to be used, subject to the provision of relevant supporting evidence (by post or email) within a specified period.

Recommendation 5: The communication strategy targeting individuals who currently hold a pseudonymous IHI should provide individuals with information (or tell them where they can find information) about:

- what they need to do if they do not have a MHR but would like to have one created;
- what they need to do (if anything) if they have a MHR.

Recommendation 6: The design of the Online Opt-Out Service channel should make it clear that an individual's reason for opting out is an optional field. Information should also be made available (whether through the MHR website or privacy policy, or the Online Opt-Out Service itself) about the purposes for which the opt-out reasons will be used by the System Operator.

In relation to the telephone and face-to-face channels, scripts for Service Centre and MHR helpline staff should also address these matters.

Recommendation 7: Consideration should be given as to whether opt-out reasons provided by an individual could be collected and retained in a de-identified form. Aside from reducing any potential risks relating to data security or other misuse, this may also address any potential privacy concerns individuals may have about providing this information.

Recommendation 8: As part of the opt-out communications (and, if possible, where an individual attempts to set their MHR privacy controls during the opt-out period), information should be provided to individuals about the effect of setting privacy controls, that is, that their MHR will become immediately available for health providers to access, subject to the individual's set privacy controls.

Recommendation 9: For the purposes of the ongoing registration arrangements, processes and system business rules should be implemented to ensure that a person is not automatically registered for a MHR where they have completed an (old) application form for Medicare enrolment or IHI assignment that is based on the opt-in model.

In these circumstances, the individual or their authorised representative should receive a confirmation that they have not been registered for a MHR, and be provided with information as to how they can apply for a MHR. This could be provided, for example, as part of the confirmation of Medicare enrolment or IHI assignment.



Recommendation 10: Before the NOO implementation commences, the Agency should commission (or review and update any existing) information security Threat and Risk Assessment in relation to the MHR system. The scope of the assessment should include consideration of:

- the bulk registration process, including in particular the transfer of data about individuals to the System Operator (NIO) and the creation of shell records at the beginning of the opt-out period, before individuals are given an opportunity to opt-out;
- cyber security threats; and
- any security risk assessments undertaken by DHS and/or the Digital Transformation Agency in relation to myGov, and how any identified risks may impact on an individual's ability to access their MHR (having regard to the increase in MHR system users under an opt-out model).

Recommendation 11: As part of the review of the complaints and incident management procedures, consideration should be given to:

- implementing appropriate systems which support accurate and consistent recording, tracking and reporting of large volumes of privacy and data security complaints and incidents; and
- ensuring an appropriate governance and management structure is in place, and that sufficient resources are allocated.

Schedule 1 – Detailed information flows: Bulk registration

The tables set out below are based on the data flow tables in Schedule 2 of the 2016 Opt-Out Trials PIA, and have been updated where relevant to reflect the data flows specific to the current design of the Bulk Registration process for the NOO Model. The third column contains comments as to whether there has been a change to the Opt-Out Trials data flows.

A. Creation of shell My Health Records for Eligible Bulk Registration (EBR) Individuals

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
Identification of EBR Individuals			
1.	Before the commencement of the opt-out period, the System Operator (NIO) requests the System Operator (DHS) to provide the HI Data Set for each EBR Individual.	N/A. (No personal information is handled in this step.)	This is a new information flow.
2.	<p>System Operator (DHS):</p> <p>a) obtains from the HI Service Operator a list of individuals who have an active verified IHI, together with the HI Data Set relating to each of those individuals;</p> <p>b) obtains from Medicare a list of individuals who should not have a record because the individual fits within one of the bulk registration eligibility exceptions (e.g. a Medicare address outside Australia, a Medicare or DVA end date, or a Medicare IRN of '0' recorded in the Medicare system).</p>	<p>HI Service Operator:</p> <ul style="list-style-type: none"> uses information in its database to identify individuals with active verified IHIs; and discloses personal information (including IHIs) about individuals to the System Operator (DHS). <p>Medicare:</p> <ul style="list-style-type: none"> uses information in the Medicare system to identify individuals who fall within one of the bulk registration eligibility exceptions; and discloses personal information about individuals to the System Operator (DHS). <p>System Operator (DHS) collects personal information from the HI Service Operator and Medicare.</p>	<p>In relation to Step 2(a), the only substantive change is that the HI Service Operator will provide HI Data Sets in relation to all individuals with an active verified IHI (i.e. not just individuals who have not opted-out).</p> <ul style="list-style-type: none"> ➤ Section 15 of the HI Act authorises the HI Service Operator to use and disclose identifying information and a healthcare identifier of a healthcare recipient for the purposes of the MHR system. ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect a healthcare identifier and identifying information about a healthcare recipient for the purposes of the MHR system. <p>Step 2(b) is a new step.</p> <ul style="list-style-type: none"> ➤ Item 5 of clause 8 of Schedule 1 to the MHR Act authorises the Chief Executive Medicare to use and disclose to the System Operator identifying information of

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
			<p>a healthcare recipient for the purposes of the MHR system.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect identifying information about a healthcare recipient to the System Operator for the purposes of the MHR system.
3.	<p>System Operator (DHS) provides the System Operator (NIO) with:</p> <ul style="list-style-type: none"> a) HI Data Sets relating to EBR Individuals; <i>[Note: System filtering rules will remove information relating to non-EBR individuals, so that the System Operator (NIO) only receives HI Data Sets in relation to EBR individuals.]</i> b) a list of trial participants who opted-out of automatic MHR registration during the 2016 Opt-Out Trials. At this time it is proposed that only IHIs will be provided (noting that the detailed design development for the bulk registration process is ongoing). 	<p>System Operator (DHS and NIO) 'use':</p> <ul style="list-style-type: none"> • personal information (including IHIs) about EBR Individuals when the System Operator (DHS) provides the HI Data Sets to the System Operator (NIO); and • personal information (specifically IHIs) about individuals who opted-out of automatic registration during the 2016 opt-out trials, <p>so that shell records are not created for individuals who are not eligible to participate in bulk registration.</p>	<p>The only substantive changes are that the System Operator (DHS) will provide to the System Operator (NIO):</p> <ul style="list-style-type: none"> • HI Data Sets in relation to all EBR Individuals, so that shell records can be created for those individuals; and • IHIs for trial participants who opted out during the 2016 Opt-Out Trials, so that the System Operator (NIO) can ensure that shell records (and later MHRs) are not created for those individuals. <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to use identifying information and a healthcare identifier of a healthcare recipient for the purposes of the MHR system.
Creation of shell My Health Record			
4.	<p>Based on the information received in Step 3, the System Operator (NIO) creates a shell record for each EBR Individual.</p>	<p>System Operator (NIO) uses personal information (including IHIs) about EBR Individuals.</p>	<p>No substantive change, except that shell records will be automatically created for all EBR Individuals before they are given opportunity to opt-out.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to use identifying information and a healthcare identifier of a healthcare recipient for the purposes of the MHR system.



B. Online Opt-Out Service

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
Accessing the Online Opt-Out Service			
5.	<p>The individual accesses the Online Opt-Out Service, and selects the option "I do not want a digital health record".</p> <p>The individual selects whether they want to opt-out for:</p> <ul style="list-style-type: none"> • themselves only; • themselves and their children; or • their children only. <p>Information about MHRs, the MHR system and the opt-out process will be made available on the myhealthrecord.gov.au website.</p> <p>The Online Opt-Out Service will be hosted by the System Operator (DHS). Information collected and stored by the System Operator (DHS) will be stored in the DHS system.</p> <p>The opt-out process commences when the individual enters their identifying information into the Online Opt-Out Service in Step 7.</p>	N/A. (No personal information is handled in this step.)	No substantive change.
6.	<p>Individuals will need to use existing processes to cancel MHRs. If an individual who already has a MHR tries to opt-out using the Online Opt-Out Service, a message will appear stating that they cannot opt-out as they already have a MHR. The page provides a link to the MHR system and the</p>	N/A.	No substantive change.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
	<p>helpline number if the individual wants to cancel their record.</p> <p><i>[Note: In the telephone and face-to-face channels, individuals will be advised if they have an existing MHR, and will be offered assistance if they wish to cancel their MHR in accordance with existing cancellation processes.]</i></p>		
Verification of individual's identity			
7.	<p>The individual enters the following information into the Online Opt-Out Service (via secure online channel):</p> <ul style="list-style-type: none"> • first and last names, sex, date of birth, and Medicare card number (including the IRN) or DVA card number; and • the unique reference number of the individual's driver licence, passport or Immicard (an 'EOI Credential') that can be verified through the Document Verification Service (DVS) and the EOI credential type. <p>This information will be collected by the System Operator (DHS), and not simply passed on to the HI Service Operator and DVS.</p>	<p>System Operator (DHS) collects personal information about the individual.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to collect identifying information of a healthcare recipient for the purposes of the MHR system.
8.	<p>System Operator (DHS):</p> <ul style="list-style-type: none"> • provides the individual's first and last names, sex, date of birth and Medicare/DVA card number to the HI Service Operator; and • requests the HI Service Operator to perform an 'IHI Lookup' and: <ul style="list-style-type: none"> ○ check the information about the individual matches the information in the HI system; and 	<p>System Operator (DHS) discloses personal information about the individual to the HI Service Operator.</p> <p>HI Service Operator collects the personal information about the individual from the System Operator (DHS).</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to disclose identifying information of a healthcare recipient for the purposes of the MHR system. ➤ Section 15 of the HI Act authorises the HI Service Operator to collect identifying information and a healthcare identifier of a healthcare recipient for the purposes of the MHR system.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
	<ul style="list-style-type: none"> ○ if there is a match, provide the individual's IHI number, IHI record status, and IHI status. <p>The above information is the minimum data set required for the HI Service Operator to identify the relevant IHI.</p>		
9.	<p>HI Service Operator checks whether there is an existing IHI record which matches the personal details provided in Step 8, and sends the IHI Lookup outcome to the System Operator (DHS).</p> <ul style="list-style-type: none"> • If there is not a unique (exact) match, the HI Service Operator sends an error message to the System Operator (DHS). • If there is a unique match, the HI Service Operator sends to the System Operator (DHS) the individual's IHI number, IHI record status, and IHI status. 	<p>HI Service Operator:</p> <ul style="list-style-type: none"> • uses the personal information collected in Step 8, as well as existing personal information held by the HI Service Operator, to locate the individual's IHI record; and • discloses personal information (including IHIs) to the System Operator (DHS). <p>System Operator (DHS) collects personal information (including IHIs) from the HI Service Operator</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to collect identifying information and a healthcare identifier of a healthcare recipient for the purposes of the MHR system. ➤ Section 15 of the HI Act authorises the HI Service Operator to use and disclose to the System Operator identifying information and a healthcare identifier of a healthcare recipient for the purposes of the MHR system.
10	<p>Following System Operator (DHS) requests DVS to perform a DVS check by providing:</p> <ul style="list-style-type: none"> • the individual's first and last names, date of birth and (where the EOI Credential is an Australia passport) sex; and • the EOI Credential type and unique reference number (and where the EOI Credential is a drivers licence, the relevant State or Territory). 	<p>System Operator (DHS) discloses personal information about the individual to the Attorney-General's Department (as the DVS operator).</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to disclose identifying information about a healthcare recipient for the purposes of the MHR system. ➤ Item 10 of clause 8 in Schedule 1 to the MHR Act provides for prescribed entities to collect, use and disclose identifying information about healthcare recipients, authorised representatives and nominated representatives for the purpose of assisting the System Operator to verify that person's identity. For the purposes of that provision, the Attorney-General's Department is prescribed in regulation 4.1.2 of the MHR Regulation.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
11	<p>DVS checks whether the individual's EOI Credential is a 'real' document (e.g. that it has a record of a driver licence, passport, etc., issued to a person matching the details provided in Step 10), and sends a 'Yes' or 'No' response to the System Operator (DHS).</p>	<p>The DVS checking process conducted by the Attorney-General's Department is out of scope for the purposes of this PIA.</p> <p>System Operator (DHS) collects the fact that the individual's identity has or has not been verified from the Attorney-General's Department (as the DVS operator).</p> <ul style="list-style-type: none"> ➤ We understand the System Operator (DHS) does not retain the details of the EOI Credential provided by the individual. It only retains the 'Yes' or 'No' response. 	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to collect identifying information about a healthcare recipient for the purposes of the MHR system. ➤ Item 10 of clause 8 in Schedule 1 to the MHR Act provides for prescribed entities to collect, use and disclose identifying information about healthcare recipients, authorised representatives and nominated representatives for the purpose of assisting the System Operator to verify that person's identity. For the purposes of that provision, the Attorney-General's Department is prescribed in regulation 4.1.2 of the MHR Regulation.
12	<p>If an error message is received from the HI Service Operator in Step 9, or a 'No' response is received from DVS in Step 11, the Online Opt-Out Service will display a message to the individual:</p> <ul style="list-style-type: none"> • advising that their identity was not verified, and recommending that they contact the helpline or a Service Centre for assistance; and • showing a Transaction Reference Number (TRN). 	<p>N/A. (No personal information is handled in this step.)</p>	<p>No substantive change.</p>
Verification of child dependants (if applicable)			
13	<p>The Online Opt-Out Service will allow the individual to specify (by entering first name and last name and IRN of) any dependants on the same Medicare card who they would like to include in the opt-out request.</p>	<p>System Operator (DHS) collects personal information about the dependants from the individual.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to collect identifying information about a healthcare recipient and an authorised representative for the purposes of the MHR system.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
14	<p>The System Operator (DHS) sends a request to Medicare for information relating to dependants listed on the individual's (hereafter, also the 'authorised representative') Medicare card.</p> <p>In making this request, the System Operator (DHS) sends to Medicare the purported Authorised Representative's first name, last name, sex, date of birth and Medicare card number (collected in Step 7) and names of dependants collected in Step 13.</p>	<p>System Operator (DHS) discloses personal information about dependants collected in Step 13 and the individual collected in Step 7 to Medicare.</p> <p>Medicare collects the information provided by the System Operator (DHS).</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to disclose identifying information about a healthcare recipient and an authorised representative for the purposes of the MHR system. ➤ Items 5 and 6 of clause 8 in Schedule 1 to the MHR Act authorise this collection by the Chief Executive Medicare from the System Operator.
15	<p>Medicare uses the individual's information to search the Medicare system and locate the dependants who:</p> <ul style="list-style-type: none"> • are listed on the same Medicare card as the individual; • are under 18 years old; and • match the information (first name, last name) entered by the individual at Step 13. <p>Medicare provides to System Operator (DHS) the Medicare card number, IRN, first name and last name and date of birth for each dependant that matches (or an error message where there is a mismatch, allowing the individual to correct and resubmit or remove the dependant in Step 13).</p>	<p>Medicare:</p> <ul style="list-style-type: none"> • uses the information provided by the System Operator (DHS), as well as existing information held in the Medicare system, to locate the dependants of the individual; and • discloses personal information about the individual's dependants to the System Operator (DHS). <p>System Operator (DHS) collects personal information about dependants (first name, last name, date of birth and Medicare card number) from Medicare.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to collect identifying information about a healthcare recipient and an authorised representative for the purposes of the MHR system. ➤ Items 5 and 6 of clause 8 in Schedule 1 to the MHR Act authorise this disclosure to the System Operator by the Chief Executive Medicare.
16	<p>System Operator (DHS):</p> <ul style="list-style-type: none"> • provides the first name, last name, sex, date of birth and Medicare number and IRN of each of the dependants identified by Medicare in Step 15 to the HI Service Operator; and • requests the HI Service Operator to perform an 'IHI Lookup' for each of the dependants. 	<p>System Operator (DHS) discloses personal information about dependants to the HI Service Operator.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to disclose identifying information about a healthcare recipient and an authorised representative for the purposes of the MHR system.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
17	<p>The HI Service Operator checks whether there is an existing IHI record which matches the personal details provided in Step 16, and sends the IHI Lookup outcome to System Operator (DHS).</p> <ul style="list-style-type: none"> If there is not an exact match, the HI Service Operator sends an error message to the System Operator (DHS). If there is an exact match, the HI Service Operator sends to the System Operator (DHS) the relevant dependants' IHI number, IHI record status and IHI status. 	<p>HI Service Operator:</p> <ul style="list-style-type: none"> collects personal information from the System Operator (DHS); uses the information collected from the System Operator (DHS), as well as existing information held by the HI Service Operator, to locate the IHI record for the relevant dependant(s); and discloses personal information (including IHIs) to the System Operator (DHS). <p>System Operator (DHS) collects personal information (including IHIs) from the HI Service Operator.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> Section 15 of the HI Act authorises the HI Service Operator to collect, use and disclosure of identifying information and a healthcare identifier of a healthcare recipient and authorised representative for the purposes of the MHR system. Item 1 of clause 8 in Schedule 1 to the MHR Act authorises the System Operator to collect identifying information and a healthcare identifier of a healthcare recipient and an authorised representative for the purposes of the MHR system.
My Health Record registration check			
18	<p>System Operator (DHS) provides the first name, last name, sex, date of birth, Medicare card number/DVA card number, IRN, IHI number, IHI record status and IHI status of the individual/Authorised Representative, and each of the dependants identified in Step 13, to the System Operator (NIO).</p> <p>System Operator (NIO) checks whether the individual/Authorised Representative, and each of the dependants identified in Step 13, is registered for a MHR and, if so, whether they have taken control of their MHR.</p> <p>After checking the MHR system, the System Operator (NIO) advises the System Operator (DHS) whether or not the individual/dependants has/have an existing MHR. Dependants who have an existing MHR and have taken control of their record will be included in the list provided to the System Operator (DHS).</p> <ul style="list-style-type: none"> As indicated in Step 6, if an individual already has a MHR, a message will appear stating that they 	<p>System Operator (DHS and NIO) 'use' personal information about the individual/Authorised Representatives and dependants in relation to the following:</p> <ul style="list-style-type: none"> System Operator (DHS) provides personal information to the System Operator (NIO); System Operator (NIO) uses the personal information received from the System Operator (DHS), as well as existing information held in the MHR system, to check whether the individual or dependant(s) have an existing MHR (and, if so, whether the dependant has taken control of their MHR); System Operator (NIO) provides the results of the check (i.e. whether there is an existing My Health Record for the individual/dependant and possibly whether the dependant has taken control of their record) to the System Operator (DHS). 	<p>No substantive change.</p> <ul style="list-style-type: none"> Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to use information and healthcare identifiers of a healthcare recipient and an authorised representative for the purposes of the MHR system.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
	cannot opt-out as they already have a MHR. The page provides a link to the MHR system and the helpline number if the individual wants to cancel their record		
Opt-Out decision			
19	System Operator (DHS) displays to the individual (via the Online Opt-Out Service) the first and last name of individuals (i.e. the individual and the dependants identified in Step 18) that can be opted-out of bulk registration. A generic message referring the individual to the telephone channel or Service Centre will be provided if an individual cannot opt-out a dependant (i.e. the message will not state if the dependant has already been opted-out or if the dependant has taken control of their own record).	System Operator (DHS) discloses personal information about dependants to the individual.	No substantive change. ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to disclose identifying information of a healthcare recipient and an authorised representative for the purposes of the MHR system.
20	<p>The individual / authorised representative:</p> <ul style="list-style-type: none"> selects the individuals they wish to opt-out of automatic bulk My Health Record registration (the 'Opt-Out Individuals'); and provides a declaration that the information they have given is true and correct and that they have parental responsibility for the dependants. <p>The individual / authorised representative may provide a reason why the individual does not want a MHR for themselves and/or their dependants before the opt-out request is finalised. The individual selects a reason from a list of six reasons. This will be an optional data field.</p> <p>This information is submitted through the Online Opt-Out Service to the System Operator (DHS).</p>	System Operator (DHS) collects personal information about the individual / authorised representative and selected dependants from the individual / authorised representative.	<p>The substantive changes are:</p> <ul style="list-style-type: none"> the Online Opt-Out Service does not prevent a shell record from being created, as this will occur prior to the commencement of the opt-out period; an individual's reason for not wanting a MHR for themselves will be obtained for purposes relating to the ongoing evaluation of, and improvements to, the MHR system (including the NOO Model) and related reporting, communications and activities. <p>The opt-out period will be a minimum of three months, but this has not yet been determined. (We note that a phased approach by jurisdiction is being considered. If adopted, it is likely that the three-month opt-out period will be provided to every jurisdiction, although these phases may overlap.)</p> <p>➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect identifying information of a</p>

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
			healthcare recipient and an authorised representative for the purposes of the MHR system.
21	<p>System Operator (DHS) stores the first name, last name, sex, date of birth, IHI number, IHI record status and IHI status of the individual of each Opt-Out Individual in the Online Opt-Out Service System.</p> <ul style="list-style-type: none"> ➤ This list will be used by the System Operator (DHS and NIO) to ensure that the shell records for Opt-Out Individuals are deleted and do not become 'live' MHRs at the end of the opt-out period. 	System Operator (DHS) collects and uses personal information about the Opt-Out Individuals.	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect, use and disclose identifying information of a healthcare recipient and an authorised representative for the purposes of the MHR system.
22	<p>A live feed will also be sent from the Online Opt-Out Service System to the System Operator (NIO) to flag an individual's shell record as having been opted-out. At this time, it is proposed that only the individual's IHI will be provided.</p>	<p>System Operator (DHS and NIO) '<u>use</u>' personal information (specifically IHIs) about individuals who have opted-out of automatic bulk registration in relation to the following:</p> <ul style="list-style-type: none"> • System Operator (DHS) provides personal information (IHIs) to the System Operator (NIO) by way of the live feed from the Online Opt-Out Service System; • System Operator (NIO) uses the personal information (IHIs) received from the System Operator (DHS) to ensure that the shell records for Opt-Out Individuals are deleted and do not become 'live' My Health Records at the end of the opt-out period. 	<p>The only substantive change is that instead of providing a list of individuals who should have a record created, the System Operator (DHS) will provide (in real-time, via the Online Opt-Out Service System) information about individuals who should <u>not</u> have a record created.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect, use and disclose a healthcare identifier of a healthcare recipient and an authorised representative for the purposes of the MHR system.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
Opt-Out Confirmation			
23	<p>System Operator (DHS) via the Online Opt-Out Service screen notifies the individual that the opt-out process was successful, which comprises the time, date and TRN of the opt-out transaction and the name, Medicare/DVA card details and (if applicable) IRN of the Opt-Out Individuals (but not any other personal information of any of the Opt-Out Individuals).</p> <p><i>Note: Where an individual opts-out through the telephone or face-to-face channels, the Service Centre or telephone helpline staff member will confirm that the opt-out has been completed at the end of the process (based on a script).</i></p>	System Operator (DHS) discloses personal information about dependants to the individual.	<p>No substantive change.</p> <p>➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to disclose identifying information about a healthcare recipient and an authorised representative for the purposes of the MHR system.</p>

C. Setting Privacy Controls

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
Setting privacy controls			
24	Individual may create and access their myGov account, and link their myGov account to their MHR.	The myGov process itself is out of scope for the purposes of this PIA. However, this PIA considers the impact of the myGov process on the ability of individuals to set their MHR privacy controls.	No substantive change.
25	<p>Individual may, at the end of the opt-out period, access their MHR through myGov, and set their access and content preferences as follows:</p> <ul style="list-style-type: none"> access preferences – if the individual wishes to limit the access by healthcare provider 	System Operator (NIO) collects personal information (i.e. information about access controls) about Automatic Registrants (i.e. Eligible Individuals who have not opted-out).	<p>No substantive change.</p> <p>➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect identifying information of a healthcare recipient for the purposes of the MHR system.</p>

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
	<p>organisations to their MHR, they can set a Record Access Code (RAC) which healthcare provider organisations must input into the MHR system in order to view the individual's MHR, or a Limited Document Access Code (LDAC) to restrict access to certain documents; and</p> <ul style="list-style-type: none"> content preferences – the individual's preferences for the inclusion of the individual's Medicare Benefits Schedule (MBS – future and past two years), Department of Veterans' Affairs (DVA – future and past two years), Pharmaceutical Benefits Scheme (PBS – future and past two years), Repatriation Pharmaceutical Benefits Scheme (RPBS – future and past two years), Australian Immunisation Register (AIR – all) and Australian Organ Donor Register (AODR – all) records into the individual's My Health Record. <p>There will be no changes to the existing access controls.</p>		<ul style="list-style-type: none"> ➤ Clause 13 of Schedule 1 of the MHR Act provides for individuals to elect not to have health information held about them by the Chief Executive Medicare disclosed to the System Operator.
26	<p>An individual can choose to set their access controls during the opt-out period.</p> <p>To do so, the individual must opt-in and have their My Health Record created in accordance with existing opt-in arrangements.</p>	<p>Existing opt-in processes are out of scope for the purposes of this PIA. However, this PIA considers the impact of limiting an individual's ability to set privacy controls before their MHR becomes available to registered healthcare provider organisations.</p>	<p>The substantive change is that an individual can only set their privacy controls during the opt-out period if they opt-in to having a MHR created for them immediately (rather than at the end of the opt-out period).</p>
27	<p>If the individual has not set their own privacy controls at the end of the opt-out period, the System Operator (NIO) sets the default access and content control settings for each Automatic Registrants' MHR, including in relation to 'standing authority' for the upload of health information and MBS and related information.</p>	<p>System Operator (NIO) uses and collects personal information (i.e. information about default access controls) about Automatic Registrants.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect, use and disclose identifying information of a healthcare recipient for the purposes of the MHR system.



D. Record Creation

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
My Health Record creation & Medicare data flow			
28	<p>At the end of the opt-out period, a MHR will be created for each EBR Individual that has not opted-out (i.e. whose shell record has not been 'flagged' as having opted-out).</p> <p>The default access and content control settings will be set for each MHR that is created.</p>	<p>System Operator (NIO) uses and collects personal information (i.e. information about default access controls).</p> <p>System Operator (DHS and NIO) 'use' personal information about individuals who have opted-out of automatic registration in relation to the following:</p> <ul style="list-style-type: none"> • System Operator (DHS) provides personal information to the System Operator (NIO); • System Operator (NIO) uses the personal information received from the System Operator to ensure that the shell records for Opt-Out Individuals are deleted and do not become 'live' My Health Records at the end of the opt-out period. 	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to collect, use and disclose identifying information of a healthcare recipient and an authorised representative for the purposes of the MHR system. ➤ Clause 3 in Schedule 1 to the MHR Act authorises the System Operator to register an eligible healthcare recipient (and create a My Health Record), provided the healthcare recipient has been given an opportunity to opt-out. New My Health Records Rules will be made to apply the opt-out model nationally.
29	<p>When either the individual or a healthcare provider accesses the individual's MHR for the first time after it is created at the end of the opt-out period, this sets off a 'trigger' to upload the two years of retrospective MBS/DVA/PBS/RPBS/AODR/ACIR data ('Medicare Data') to the individual's MHR. (In the case of the healthcare provider, the type of 'access' would be a user viewing the MHR.)</p>	N/A. (No personal information is handled in this step.)	No substantive change.
30	<p>An electronic notification is sent from the System Operator (NIO) to the Chief Executive Medicare (registered repository operator) to request that</p>	<p>System Operator (NIO) discloses personal information to the Chief Executive Medicare.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act authorises the System Operator to disclose identifying

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
	<p>Medicare Data be made available in the MHR system. The request will include the following information about the individual:</p> <ul style="list-style-type: none"> • IHI; • whether the individual has a MHR identity and/or MHR; and • the Medicare Data to be made available (based in the individual's content preferences, if any). 		<p>information of a healthcare recipient for the purposes of the MHR system.</p> <ul style="list-style-type: none"> ➤ Item 7 of clause 8 of Schedule 1 to the MHR Act authorises the collection by Chief Executive Medicare. ➤ Clause 12 of Schedule 1 to the MHR Act authorises the Chief Executive Medicare to disclose health information held by the Chief Executive Medicare about an individual to the System Operator where the individual has not opted-out of this.
31	<p>The Chief Executive Medicare (registered repository operator) identifies the Medicare record for the individual in the Medicare/DVA claims database, PBS/RPBS claims database and ACIR and AODR (the 'live system') using the IHI.</p>	<p>The Chief Executive Medicare uses personal information about an individual.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 7 of clause 8 of Schedule 1 to the MHR Act authorises the use by Chief Executive Medicare.
32	<p>The Chief Executive Medicare (registered repository operator) copies the individual's MBS/DVA claims records, PBS/RPBS records, ACIR records and AODR records from its live system to its MHR repository administration system.</p>	<p>The Chief Executive Medicare uploads information about an individual to its MHR repository administration system.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Clause 11 of Schedule 1 to the MHR Act authorises the Chief Executive Medicare to upload information about an individual to its MHR repository administration system.
33	<p>The Chief Executive Medicare (registered repository operator) attaches the individual's IHI to the individual's Medicare Data in its MHR repository administration system.</p>	<p>The Chief Executive Medicare uses personal information about an individual.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 7 of clause 8 of Schedule 1 to the MHR Act expressly authorises the use by Chief Executive Medicare.

Step	Description	Information flow	Changes to information flow compared to Opt-Out Trial
34	<p>The Chief Executive Medicare (registered repository operator) sorts the records in its MHR repository administration system to match the automatic (default) uploading of Medicare Data.</p> <p>The Chief Executive Medicare (registered repository operator) indexes the records for individuals who have not opted-out of having their retrospective Medicare Data from being uploaded. A list of key fields for each record is created in the repository.</p>	<p>The Chief Executive Medicare uses personal information about an individual.</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 7 of clause 8 of Schedule 1 to the MHR Act authorises the use by Chief Executive Medicare.
35	<p>The Chief Executive Medicare (registered repository operator) makes the index available to the System Operator (NIO).</p>	<p>The Chief Executive Medicare discloses personal information about an individual to the System Operator (NIO).</p>	<p>No substantive change.</p> <ul style="list-style-type: none"> ➤ Item 1 of clause 8 of Schedule 1 to the MHR Act expressly authorises the System Operator to collect, use and disclose identifying information of a healthcare recipient for the purposes of the MHR system. ➤ Clause 12 of Schedule 1 and Item 7 of clause 8 of Schedule 1 to the MHR Act authorises the use and disclosure by Chief Executive Medicare. ➤ Clause 7 of Schedule 1 also authorises collection of health information by the System Operator for inclusion in the My Health Record of a recipient.

Schedule 2- Sources of information

Publicly available information

My Health Record related documents / information

- Deloitte, *Report to the Commonwealth Department of Health on the public consultation into the implementation of the recommendations of the Review of the Personally Controlled Electronic Health Record (September 2014)* (available at [http://www.health.gov.au/internet/main/publishing.nsf/content/17BF043A41D470A9CA257E13000C9322/\\$File/Report%20-%20Consultation%20on%20PCEHR%20Review%20Recommendations%20-%20Sep2014.pdf](http://www.health.gov.au/internet/main/publishing.nsf/content/17BF043A41D470A9CA257E13000C9322/$File/Report%20-%20Consultation%20on%20PCEHR%20Review%20Recommendations%20-%20Sep2014.pdf))
- MinterEllison, *Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model (20 May 2015)*, prepared for the Department of Health (available at [https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/faq-security-410/\\$file/PCEHR%20Opt%20Out%20PIA%20-%202015.pdf](https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/faq-security-410/$file/PCEHR%20Opt%20Out%20PIA%20-%202015.pdf))
- My Health Record System Operator Privacy Policy (updated on 5 December 2016) (available at <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/privacy-statement>)
- Review Panel, *Review of the Personally Controlled Electronic Health Record* (December 2016) (available at <http://delimiter.com.au/wp-content/uploads/2014/05/FINAL-Review-of-PCEHR-December-2013.pdf>)
- Siggins Miller, *Evaluation of the Participation Trials for the My Health Record: Final Report (November 2016)* (available at <http://www.health.gov.au/internet/main/publishing.nsf/Content/ehealth-evaluation-trials>)

OAIC documents

- *Australian Privacy Principles Guidelines* (as at 1 April 2015)
- *Community Attitudes to Privacy survey: 2013 Research Report*
- *Guide to securing personal information: 'Reasonable steps' to protect personal information* (January 2015)
- *Privacy Impact Assessment Guide* (May 2014).

Agency information

- *Brief to Advise for the PIA*
- Statistics on MHR privacy complaints and privacy breaches (provided by the Agency on 20 June 2017)
- *Opt-Out Participation in the My Health Records System – Proposed process* (updated as at 28 April 2017).

Other documents and information provided by the Agency

- Ashurst, *Privacy Impact Assessment: My Health Record – Opt-Out Trials* (draft version 8 dated 21 March 2016), prepared for the Department of Health
- Department of Health, *Drafting instructions for My Health Records (National Opt-out) Rule* (12 April 2017) (provided by the Agency on 2 May 2017)
- Information Integrity Solutions, *Privacy advice in relation to My Health Record creation* (1 December 2016), prepared for the Department of Health



Legislation

- *Healthcare Identifiers Act 2010 (Cth)*
- *Healthcare Identifiers Regulations 2010 (Cth)*
- *My Health Records Act 2012 (Cth)*
- *My Health Records Regulation 2012 (Cth)*
- *My Health Records Rule 2016 (Cth)*
- *My Health Records (Assisted Registration) Rule 2015*
- *My Health Records (Opt-out Trials) Rule 2016 (Cth)*
- *Privacy Act 1988 (Cth)*

Schedule 3– Glossary and acronyms

Term or Acronym	Meaning
2015 PIA	MinterEllison, <i>Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model (20 May 2015)</i> , prepared for the Department of Health (available at https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/faq-security-410/\$file/PCEHR%20Opt%20Out%20PIA%20-%202015.pdf).
2016 PIA	Ashurst, <i>Privacy Impact Assessment: My Health Record – Opt-Out Trials</i> (draft version 8 dated 21 March 2016), prepared for the Department of Health.
2016 Privacy Advice	Information Integrity Solutions, <i>Privacy advice in relation to My Health Record creation</i> (1 December 2016), prepared for the Department of Health.
AIR	Australian Immunisation Register, a national register administered by DHS that captures all vaccines administered throughout a person's life (i.e. birth to death), given through general practice and community clinics. This will include all vaccines funded under the National Immunisation Program, and may also include private vaccines given through general practice and community clinics.
Agency	Australian Digital Health Agency
AODR	Australian Organ Donor Register, the national register for organ and tissue donation for transplantation. The AODR keeps a record of the individual's donation decision and the organ/tissue the individual agrees to donate.
APPs	Australian Privacy Principles, as set out in Schedule 1 of the Privacy Act
APP Guidelines	The <i>Australian Privacy Principles Guidelines</i> , prepared by the Australian Information Commissioner under section 28 of the Privacy Act.
authorised representative	An 'authorised representative' of a healthcare recipient as defined in section 6 of the MHR Act.
Chief Executive Medicare (Repository Operator)	The Chief Executive Medicare, acting through delegated officers of DHS, and performing the functions of a registered repository operator under section 38 of the MHR Act.
Deloitte Report	Deloitte, <i>Report to the Commonwealth Department of Health on the public consultation into the implementation of the recommendations of the Review of the Personally Controlled Electronic Health Record (September 2014)</i> (available at http://www.health.gov.au/internet/main/publishing.nsf/content/17BF043A41D470A9CA257E13000C9322/\$File/Report%20-%20Consultation%20on%20PCEHR%20Review%20Recommendations%20-%20Sep2014.pdf)
DOH	Department of Health
DHS	Department of Human Services
DVA	Department of Veterans' Affairs
EBR Individual	Eligible bulk registration individual, i.e. an individual who is eligible to participate in the bulk opt-out registration process.
EOI	Evidence of Identity
Evaluation Report	Siggins Miller, <i>Evaluation of the Participation Trials for the My Health Record: Final Report (November 2016)</i> (available at http://www.health.gov.au/internet/main/publishing.nsf/Content/ehealth-evaluation-trials).

Term or Acronym	Meaning
healthcare recipient	An individual who has received, receives or may receive healthcare (as defined in section 5 of the MHR Act).
Health Insurance Act	<i>Health Insurance Act 1973</i> (Cth)
HI Act	<i>Healthcare Identifiers Act 2010</i> (Cth)
HI Data Set	An individual's first name, last name, sex, IHI number, IHI record status, date of birth and address.
HI Service	A service that enables unique identifiers to be created for individuals and healthcare providers across the Australian healthcare system.
HI Service Operator	The 'service operator' as defined in section 6 of the HI Act, being the Chief Executive Medicare (acting through delegated DHS officers).
HPI-I	A 16-digit unique number assigned to healthcare provider individuals, which is used to identify individual providers who deliver healthcare in the Australian healthcare setting.
HPI-O	A 16-digit unique number assigned to healthcare provider organisations, which is used to identify organisations who deliver healthcare in the Australian healthcare setting.
IHI	A 16-digit unique number assigned to members of the public, which is used to identify individuals who receive healthcare in the Australian healthcare setting. There are five types of IHI status: active, deceased, retired, expired and resolved. There are three types of IHI record status: verified, unverified and provisional.
IRN	Individual Reference Number (shown on a Medicare card)
MBS	Medicare Benefits Schedule
Medicare	Chief Executive Medicare acting through delegated DHS officers in the performance of Medicare-related functions under the National Health Act and the Health Insurance Act.
Medicare Data	Two years of retrospective MBS, PBS, DV, RPBS, ACIR and AODR data relating to an individual.
MHR	My Health Record
MHR Act	<i>My Health Records Act 2012</i> (Cth)
MHR Regulation	<i>My Health Records Regulation 2012</i> (Cth)
MHR system	My Health Record system
MHR website	myhealthrecord.gov.au
Minister	Federal Minister for Health
National Health Act	<i>National Health Act 1953</i> (Cth)
NIO	National Infrastructure Operator
NOO model	National Opt-Out model
OAIC	Office of the Australian Information Commissioner
Online Opt-Out Service	The online service to be used by individuals to indicate that they do not want to be automatically registered for a MHR.
opt-out period	The period during which individuals can opt-out of automatic bulk registration for a MHR.

Term or Acronym	Meaning
Opt-Out Trials	The trials of an opt-out model for MHR registration, which were held between March and October 2016 at trial sites in Northern Queensland and the Nepean Blue Mountains of New South Wales
Opt-Out Trials Rule	<i>My Health Record (Opt-out Trials) Rule 2016</i> (Cth)
participant in the MHR system	A 'participant in the My Health Record system' as defined in section 5 of the MHR Act
PBS	Pharmaceutical Benefits Scheme
PCEHR	Personally Controlled Electronic Health Record
PHN	Primary Health Network
Previous Privacy Assessments	Collective reference to the 2015 PIA, 2016 PIA and 2016 Privacy Advice
Privacy Act	<i>Privacy Act 1988</i> (Cth)
registration	The process associated with the creation of a MHR
RPBS	Repatriation Pharmaceutical Benefits Scheme
Service Centre	Physical premises where an individual can seek assistance and make inquiries in relation to the MHR system, including the opt-out process. A Service Centre could be staffed by DHS or a third party provider contracted by the Agency, depending on the arrangements for the performance of MHR functions and activities at a particular time.
System Operator	The 'System Operator' as defined in section 14 of the MHR Act. Pursuant to paragraph 14(1)(b) and regulation 2.1.1 of the MHR Regulations, the Agency has been the System Operator since July 2016.
System Operator (DHS)	DHS as delegate of the System Operator
System Operator (NIO)	The System Operator acting through NIO as its contracted service provider