Australian Government

Australian Digital Health Agency

OFFICIAL

Appendix A – Implementation scope for ANAO recommendations

A.1 Recommendation 1

A.1.1 Background

- Ten reports were commissioned by Health or the Agency to assess privacy risks of My Health Record between December 2011 and July 2017, focussing on various aspects of the system design and operation.
- An information security assessment of the system in 2016 identified risks with variable healthcare provider awareness of privacy and security.
- Between 2011 and 2017, the OAIC undertook 14 privacy assessments in relation to the My Health Record system and the Healthcare Identifiers Service. Five assessments were conducted between 2017/18 and 2018/2019 and an additional two are due to commence in 2019/20. No assessments have been delivered to the Agency since 2017.
- Two Senate committee inquiries considered privacy risks in the My Health Record system.
- Agency risk registers currently identify some shared risks with other entities, however more clarity on roles and responsibilities of shared risks in both government and non-government entities is required.

A.1.2 Success Criteria

- The Agency documents an overarching privacy risk assessment of the My Health Record system, including any shared risks.
- The privacy risk assessment and appropriate controls are incorporated into the risk management framework for the My Health Record system. Treatments should focus on reducing potential harm to individuals and the community.
- Shared risks will be identified and monitored through appropriate information exchanges between relevant government and non-government stakeholders.
- Responsibility for monitoring shared risks and implementing controls are agreed and documented by relevant parties through a collaborative process. Reporting mechanisms are established to identify any new privacy risk exposure.

A.1.3 High level implementation plan

No.	Activity	Description
1	Context	• Review all documented risks already identified in completed MHR privacy risk assessments. • Map stakeholders to understand which organisations the Agency may share privacy risks. • Consider objectives of all organisations and how these may result in shared risks. • Identify existing mechanisms, such as committees, which may already be managing shared risk.
2	Engagement	• Engage privacy risk assessment service provider to bring independent assurance and a holistic view in developing the privacy risk assessment, including shared risks. • Conduct joint workshops with stakeholders to identify shared risks.
3	Risk analysis and evaluation	• Consider how the same risk can affect entities with different objectives and measures of success in different ways. • Consider risk severity from the perspective of each party, and to the community as a whole. • Consider cascading impacts between entities, where, for example, realising the risk may affect the ability of a third party to contribute to its management, further increasing its affects. • Consider the risk appetite of each contributing third party when evaluating the tolerability of a risk.
4	Risk treatments	• Determine and document third party responsibilities for risk controls and treatments. Ensure third parties clearly understand their treatment responsibilities, even if they've not been involved in the risk assessment. • Establish inter-entity arrangements, or mechanisms to coordinate the application of various controls and treatments. • Determine and document responsibilities for monitoring, reporting and assuring the implementation of controls and treatments.
5	Communication and Monitoring	• Ensure all parties clearly understand their exposure to the risk. • Establish reporting frameworks to ensure assurance mechanisms and risk indicators are not forgotten over time. • Incorporate shared risk reporting into the existing governance reporting arrangements of third parties. • Incorporate the results of the privacy risk assessment outcomes into the MHR risk management framework

Content informed by Department of Finance – shared risk guidance https://www.finance.gov.au/sites/default/files/2019-11/comcover-information-sheet-understanding-and-managing-shared-risk.pdf

Recommendation 1 – High level implementation plan												
	2020											
Activity	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Context		▨	▨	▨								
Engagement				▨	▨	▨	▨					
Risk analysis and evaluation							▨	▨	▨			
Risk treatments									▨	▨	▨	
Communication and monitoring											▨	▨

A.1.4 High level outputs

- Collaborative engagement with third parties to:
  - identify shared risks and accountabilities
  - nominate transparent roles and responsibilities
  - define risk appetite boundaries, and
  - agree on appropriate governance, controls and treatments of the risks.
- Incorporate shared risks into an end-to-end privacy risk assessment of the My Health Record system.
- Incorporate the results of the end-to-end privacy risk assessment into the risk management framework for the My Health Record system.
- Monitoring of treatments and controls, including risks that are shared with third parties
- ***Note:*** *An overview of how the Agency will develop assurance over third-party software connections is discussed under recommendation 3.*

A.2 Recommendation 2

A.2.1 Background

- Section 64 of the *My Health Records Act 2012* authorises a participant in the system to use the 'emergency access' function to override a healthcare recipient's access controls. This function must only be used in circumstances involving a serious threat to an individual's life, health or safety, or a serious threat to public health or public safety.
- The Agency monitors the use of this function. The Agency has previously written to healthcare provider organisations for more information about the circumstances of using this function. To date the Agency has not taken additional steps to address any potential interferences with privacy as a result of an incorrect use of this function.
- Only 8.2 per cent of instances where the emergency access function was used involved accessing the My Health Record of a healthcare recipient that had applied access controls. Nevertheless, the remaining 92 per cent of instances where emergency access was used are still required to be justified as there is no indication whether a consumer has hidden some documents prior to using the emergency access function.

A.2.2 Success Criteria

- That the Agency delivers a digital health regulatory compliance framework that gives confidence to the Parliament, Government, stakeholders and the community.
- The framework provides participants in the My Health Record system, and other digital health initiatives, with a clear understanding on how the Agency monitors third party compliance with legislative obligations.
- The Agency's regulatory compliance framework will facilitate interaction with My Health Record and digital health activities whilst also mitigating risks posed to the community.
- An independent review of the compliance regime is completed after one year of operation. This review will determine whether Agency activities are achieving the desired objectives, including potential for harm is minimised and whether the associated benefits and impacts for regulated entities and the community are appropriate.

A.2.3 High level outputs

- Implement an approach to monitor the use of the emergency access function authorised under section 64 of the My Health Records Act.
- Compliance activities are designed to be scalable so the System Operator can address other potential non-compliance activities under the My Health Records Act, as well as other digital health initiatives.
- Consult with relevant stakeholders, including the Department of Health and the OAIC, when designing a regulatory compliance approach for My Health Record and digital health. Consideration should be given to:
    - The appropriateness of a risk-based approach to regulatory compliance. This will assist the Agency address high risk activities and patterns of non-compliance while effectively allocating resources.
    - Including a base level of compliance management activities to monitor registering healthcare provider organisations and contracted service provider compliance.

- The different regulatory compliance strategies to address the different risks posed to individuals and the community. In particular, the role of the Information Commissioner as the regulator of privacy aspects of the My Health Record system must be considered in developing any regulatory compliance framework.
- How regulated entities will be provided with a clear awareness and understanding of their compliance obligations.
- Whether compliance activities are achieving the objectives and provide an avenue to identify any adverse impacts on the community, healthcare providers or contracted service providers.
- How data analysis (where available) can be used to monitor non-compliance, risk and to identify trends or behaviours which can be an indicator of non-compliance.
- Minimising information requests to the minimum necessary to monitor compliance effectively. Duplication of requests from other regulators, accreditation providers or the Agency should be avoided.

A.2.4 High level implementation plan

No.	Activity	Description
1	Context	• Review existing compliance and assurance activities performed by the Agency. • Map stakeholders to understand which organisations may be impacted by any proposed compliance and assurance activities. • Discuss potential regulatory approaches with the Department of Health and the OAIC
2	Engagement	• Meet with relevant participants to determine their understanding of (and ability to comply with) the relevant sections of the MHR Act and MHR Rules. • Document the regulatory behaviour of participants through these interactions • Test the different regulatory compliance approaches that could be applied to participants through this process
3	Regulatory design	• Design an appropriate regulatory approach in consultation with the Department of Health and the OAIC
4	Consultation and refinement	• Consult with regulated entities about the proposed regulatory compliance framework • Refine the approach where appropriate
5	Implementation and review	• Implement the regulatory compliance framework • Independent review completed to determine if Agency activities are achieving the desired objectives

Recommendation 2 – High level implementation plan												
	2020											
Activity	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Context		▨	▨									
Engagement				▨	▨	▨						
Regulatory design						▨	▨	▨	▨			
Consultation/refinement									▨	▨	▨	
Implementation/review											▨	▨

A.3 Recommendation 3

A.3.1 Background

The existing assurance processes (for HI Service and My Health Record) consists of;

- Pre-production connection testing for both HI Service and My Health Record,
- NATA accredited product testing for the HI Service, and
- self-assessment of My Health Record functionality confirmed via a declaration of conformity.

In 2020 the My Health Record mobile gateway will reopen to vendors and this will also include conformance & assurance activities which will be within scope of this recommendation.

The assurance process also consists of analysis of production data uploaded to the My Health Record system once a product is connected.

The Agency also conducts assurance activities in other work programs such as secure messaging and electronic prescribing.

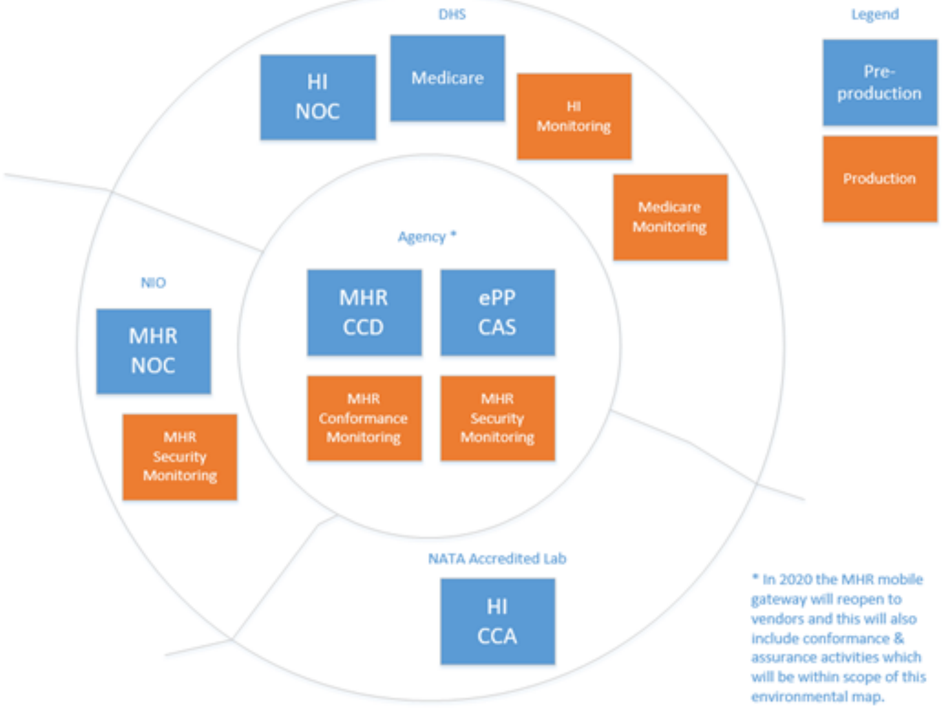
The combination of these existing assurance activities is not specifically defined within a single assurance framework.

When contemplating changes to assurance it is important to have a strong understanding of the balance between security/privacy and adoption. For example, creating new barriers for software vendors to connect to the My Health Record may reduce the likelihood of their connection. It is possible that this hurdle will be overcome in the future once My Health Record reaches a tipping point in adoption, this timeline may help to guide when applicable changes should be made to assurance processes.

A.3.2 Success Criteria

- An assurance framework will be delivered which describes software assurance processes for software connecting to the My Health Record. This framework will take into consideration the Information Security Manual for alignment.
- Improvements to the Agency’s assurance processes should ultimately result in improved standards in the health software industry, including but not necessarily limited to their interactions with the My Health Record.
- The resulting assurance framework should meet the expectations of the community in delivering a balanced approach to effort while meeting technical, security and privacy concerns of users.
- Any changes to product assurance should undergo consultation with industry participants such as software vendors, industry associations and state jurisdictions. Other industry participants will be involved depending on the scope and scale of changes, i.e. Department of Human Services, standards organisations, etc.
- Changes to the assurance process should not introduce significant negative change in the health software industry. These may include such circumstances as creating unfair market advantage, limiting competition between software vendors, impeding on health care provider choice when selecting software, or the usability of health software.

A.3.3 Technology assurance environmental map (current state)



* In 2020 the MHR mobile gateway will reopen to vendors and this will also include conformance & assurance activities which will be within scope of this environmental map.

A.3.4 High level outputs

Output 1: Baseline digital health assurance framework

The recommendation suggests to develop an assurance framework which aligns with the Information Security Model. The Agency’s existing assurance processes will be amalgamated into a single framework to define the current state, which can act as a baseline for future improvements.

- This will include the Agency’s conformance activities for the My Health Record system, Secure Messaging, Electronic Prescribing, and any other applicable work programs.
- The framework will incorporate Agency process regarding pre-production assessment, in-production analytics & monitoring, rectification of identified issues.
- The framework will include supplementary information describing external assurance activities within a defined scope. This scope would likely include the HI Service and Medicare although would be a subset derived from the ***Technology assurance environmental map*** above and decided by key stakeholders during initial engagement activities.

Output 2: Health software industry assurance roadmap

Industry participants and government stakeholders will be engaged to assess future alignment with the Information Security Manual and develop a health software industry assurance roadmap. This roadmap will take into consideration the effect that heightened requirements will have on My Health Record adoption. Other national infrastructure and functionality such as Medicare Billing and Electronic Prescribing may also benefit from a standardised assurance model and could prove integral in adoption by the health software sector.

- The ANAO recognised that any ISM assurance process must be balanced against disincentives to register and use the system (3.75).
- The existing digital health assurance framework will be used as a baseline to map against the Information Security Manual and develop a list of priorities for the health software sector.

The roadmap will define timelines for integration of agreed upon changes to the assurance framework.

A.3.5 High level implementation plan

No.	Activity	Description
1	External engagement for baseline and assurance roadmap	• External resources from DHS, Health, jurisdictions, MSIA, standards associations and industry participants would be included. • The goal would be to define the scope of the assurance framework roadmap, and once the scope is confirmed, to attain the applicable assurances processes to include as supplementary documents in the baselined digital health assurance framework.
2	Internal engagement for baseline and assurance roadmap	• Internal resources from Innovation, Implementation & Support, Mobility, Electronic Prescribing, Conformance, MHR Product, Policy, Privacy, Security & Operations. • This engagement would likely focus on two activities; • Documenting existing assurance processes into a framework • Discussing priorities and industry adoption to plan the digital health assurance roadmap
3	Baseline assurance framework delivery	• This deliverable identifies the current state of assurance within the Agency and across other external assurance activities which are considered in scope. • Describe alignment with the Information Security Manual where it exists.
4	Agree priorities and method of implementation	• The relevant stakeholders will agree upon a list of priorities for health software vendors to implement within their products and possible incentives.
5	Health software industry Assurance Roadmap delivery	• As per the high level output above, the industry assurance roadmap will be an industry agreed list of changes to be implemented over a specific timeframe, taking into consideration the balance between adoption and security/privacy.

Recommendation 3 – High level implementation plan												
Activity	2020											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
External engagement		■	■									
Internal engagement			■	■	■							

Baseline framework						■						
Prioritise roadmap							■	■	■			
Roadmap delivery										■	■	■

A.4 Recommendation 4

A.4.1 Background

- Part 5, Division 3 and 4 of the *My Health Records Rule 2016* requires healthcare provider organisations and contracted service providers to comply with mandatory legislated security requirements in order to be eligible, and remain eligible, for registration.
- Mandatory legislated security requirements include having a written security policy in place, user account management requirements, and the protection of record codes and document codes.
- The Agency has previously reviewed a small sample of GPs against the requirement to have a security policy in place. This review found only 32 per cent of survey recipients fully met this requirement.

A.4.2 Success Criteria

- That the Agency delivers a digital health regulatory compliance framework that gives confidence to the Parliament, Government, stakeholders and the community.
- The framework provides participants in the My Health Record system, and other digital health initiatives, with a clear understanding on how the Agency monitors third party compliance with legislative obligations.
- The Agency's regulatory compliance framework will facilitate interaction with My Health Record and digital health activities whilst also mitigating risks posed to the community.
- An independent review of the compliance regime is completed after one year of operation. This review will determine whether Agency activities are achieving the desired objectives, including potential for harm is minimised and whether the associated benefits and impacts for regulated entities and the community are appropriate.

A.4.3 High level outputs

- Implement a compliance assurance approach to monitor healthcare provider organisation and contracted service provider security requirements, as outlined in MHR Rule Part 5 Division 3 and 4.
- Compliance activities are designed to be scalable so the System Operator can address general registration requirements. This includes those in Part 5 Division 1 and 2 of the MHR Rule, the My Health Records Act, as well as other digital health initiatives.
- Consult with relevant stakeholders, including the Department of Health and the OAIC, when designing a regulatory compliance approach for My Health Record and digital health. Consideration should be given to:
    - The appropriateness of a risk-based approach to regulatory compliance. This will assist the Agency address high risk activities and patterns of non-compliance while effectively allocating resources.
    - Including a base level of compliance management activities to monitor registering healthcare provider organisations and contracted service provider compliance.
    - The different regulatory compliance strategies to address the different risks posed to individuals and the community. In particular, the role of the Information Commissioner as the regulator of privacy aspects of the My Health Record system must be considered in developing any regulatory compliance framework.

- How regulated entities will be provided with a clear awareness and understanding of their compliance obligations.
- Whether compliance activities are achieving the objectives and provide an avenue to identify any adverse impacts on the community, healthcare providers or contracted service providers.
- How data analysis (where available) can be used to monitor non-compliance, risk and to identify trends or behaviours which can be an indicator of non-compliance.
- Minimising information requests to the minimum necessary to monitor compliance effectively. Duplication of requests from other regulators, accreditation providers or the Agency should be avoided.

A.4.4 High level implementation plan

No.	Activity	Description
1	Context	• Review existing compliance and assurance activities performed by the Agency. • Map stakeholders to understand which organisations may be impacted by any proposed compliance and assurance activities. • Discuss potential regulatory approaches with the Department of Health and the OAIC
2	Engagement	• Meet with relevant participants to determine their understanding of (and ability to comply with) the relevant sections of the MHR Act and MHR Rules. • Document the regulatory behaviour of participants through these interactions • Test the different regulatory compliance approaches that could be applied to participants through this process
3	Regulatory design	• Design an appropriate regulatory approach in consultation with the Department of Health and the OAIC
4	Consultation and refinement	• Consult with regulated entities about the proposed regulatory compliance framework • Refine the approach where appropriate
5	Implementation and review	• Implement the regulatory compliance framework • Independent review completed to determine if Agency activities are achieving the desired objectives

Recommendation 4 – High level implementation plan												
	2020											
Activity	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Context		▨	▨									
Engagement				▨	▨	▨						
Regulatory design						▨	▨	▨	▨			
Consultation/refinement									▨	▨	▨	
Implementation/review											▨	▨

A.5 Recommendation 5

A.5.1 Background

- In 2017 a benefits realisation plan estimated the benefits of MHR over 10 years and has not yet been revised.
- Broadly benefits were modelled around intermediate and longer-term time frames and more granularity is considered important
- Ongoing research activities to support measuring benefits realisation has been commissioned.

A.5.2 Success Criteria

- That the Agency finalises the in-flight Benefits Measurement and Management Plan to reflect a 10 year stage plan, ensuring key benefits milestones and dependencies for achieving these are clearly outlined.
- Assumptions concerning the feasibility and sequencing of dependencies for achieving benefits milestones are the subject of consultation with key collaborators internally and externally.
- Limitations to benefits modelling are shared to set expectations around the likelihood of achievement. This will inform strategies to respond incrementally where realisation of benefits milestones is at risk.
- Progress towards benefits realisation will be data driven and reported according to agreed governance.
- Ensure benefits milestones will be staged to support the incremental roll out of the compliance and assurance framework for third party software and monitoring of mandatory legislated security requirements.

A.5.3 High level outputs

Consultation Plan

- Engage the newly formed Insights and Analytics, and Research and Evaluation Teams to align internally the objectives of the Benefits Measurement and Management Plan to incorporate requirements of the audit. This will inform external engagement as described above under A.5.4.

Benefits Measurement and evaluation plan

- To ensure delivery of the longer term (10 year) Benefits Measurement and Management Plan, seek formal agreement of underpinning metrics and performance indicators from the Commonwealth Department of Health.
- Ensure each of the defined forward timeframes in the plan can inform the sequencing of projected benefits to enable maturity of Reporting and Compliance workstream.

Support of third-party analytics and research

- Ongoing specialist analytics and research will be commissioned to apply agreed metrics and performance indicators. Support will extend to transparent procurement of these services to ensure best of breed analytics and research informs communication about benefits realisation.

Availability of unit record level data access (data provisioning)

- To achieve a granularity of reporting against metrics and performance indicators, access to unit record level data (to support linkage with MHR data) is required, de-identified for the purposes of appropriate provisioning of that data. This work will require a maturity of governance concerning secondary use to be understood and recognised as a formal dependency for reporting on benefits realisation.
- Specific deliverables include advice on limits on use of health information for benefits analytics under MHR legislation and where the secondary use framework is underpinned by operational maturity needs to be applied.

A.5.4 High level implementation plan

No.	Activity	Description
1	Context	• Benefits measurement and evaluation plan (short form) will require amendment to reflect a 10-year milestone plan and act as the My Health Record evaluation plan reflected in the recommendation.
2	Engagement	• Meet with relevant parties to determine a way forward to provision of unit record data to support analytics in the form of MHR and other health data linkage. • Following agreement from the Commonwealth Department of Health, share metrics and performance indicators underpinning benefits modelling with impacted stakeholders. • Share and align benefits reporting approach.
3	Consultation and refinement	• Consult with entities supplying to or impacted by the benefits evaluation plan and test actual and 'stretch' components of the planned approach • Refine the approach where appropriate.
4	Implementation and review	•

Recommendation 5 – High level implementation plan

	2020											
Activity	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Context	▨	▨										
Engagement		▨	▨	▨	▨							
Consultation and refinement					▨	▨	▨	▨				
Implementation and review							▨	▨	▨	▨	▨	▨