A review of the

# Safety and Quality Benefits of Secure Messaging

Australian Government
Australian Digital Health Agency

AUSTRALIAN COMMISSION ON SAFETY AND QUALITY IN HEALTH CARE

**Australian Digital Health Agency**
ABN 84 425 496 912 | Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

**Acknowledgements**

The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

**Disclaimer**

The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

**Document control**

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

**Copyright© 2020 Australian Digital Health Agency**

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

**Product or document version history**

Product or document version: v1.0
Date: November 2020
Release comments: Initial publication

**OFFICIAL**

# Contents

# About the Australian Digital Health Agency

The Agency is tasked with improving health outcomes for all Australians through the delivery of digital healthcare systems, and implementing *Australia's National Digital Health Strategy – Safe, Seamless, and Secure: evolving health and care to meet the needs of modern Australia* in collaboration with partners across the community. The Agency is the System Operator of My Health Record, and provides leadership, coordination, and delivery of a collaborative and innovative approach to utilising technology to support and enhance a clinically safe and connected national health system. These improvements will give individuals more control of their health and their health information, and support healthcare providers to deliver informed healthcare through access to current clinical and treatment information. Further information: www.digitalhealth.gov.au

# About the Australian Commission on Safety and Quality in Health Care

The Commission works in partnership with patients, carers, clinicians, the Australian state and territory health systems, the private sector, managers and healthcare organisations to achieve a safe, high-quality and sustainable health system.

The Australian Digital Health Agency appointed the Commission to undertake a clinical safety program for the My Health Record. The Program contributes to improving the clinical quality, safety and utility of national digital health infrastructure and the aims outlined in the National Digital Health Strategy (NDHS) 2018–22. Findings and recommendations resulting from the Program inform future development and system improvements of national digital health infrastructure.

# Why is secure messaging important?

The need for a connected healthcare system has never been greater. The impact of COVID-19 has highlighted the need for healthcare providers to connect with each other in a safe and secure digital environment.

Secure messaging is an efficient and timely method for sending and receiving clinical information, which minimises the burden of paper and manual processes.

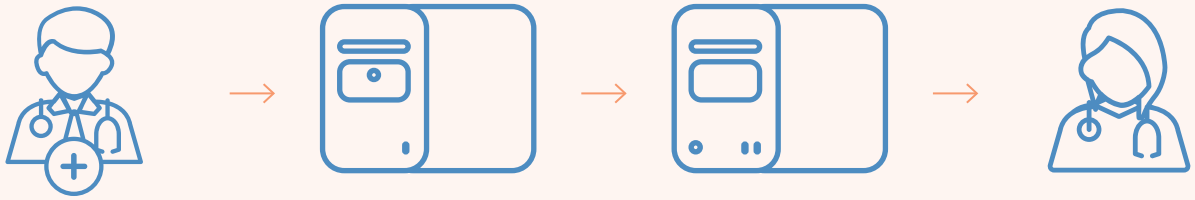
An increased uptake of secure messaging improves continuity of care for patients, saves time and protects vital health information.

Secure messaging is a crucial step forward in our journey to better health for all Australians.

# Background

Secure messaging systems allow healthcare professionals to send health information securely to other healthcare professionals involved in their patients' care. The exchange of health information is typically conducted via the healthcare professionals' clinical information system. Secure messaging is regarded as a 'point-to-point' exchange, which is distinct to the 'point-to-many' exchange used by electronic health records such as the My Health Record.

**Figure 1:**
Typical example of secure messaging




Secure provider-to-provider communication is a key component of digitally-enabled integrated and coordinated care across the Australian healthcare system. Secure messaging provides foundational capability to enable safe, seamless and secure information sharing across healthcare providers and consumers.

There are exemplars of secure messaging use, such as pathology reports and discharge summaries from hospitals to other healthcare providers. However, there continues to be an inconsistent approach to secure messaging. This has contributed to information exchange challenges experienced by clinicians across the system.

Secure Message Delivery is a set of specifications that defines an approach to digital health communication using widely supported IT industry standards. The specifications support the secure delivery either of messages containing clinical documents and/or other information between healthcare organisations, directly or through one or more messaging service providers. A typical example is outlined in Figure 1.

In addition to having a secure messaging connection, sending and receiving clinical information systems need to be conformant to document format standards. The Agency has defined Clinical Document Architecture (CDA) standards for discharge summaries, eReferrals and specialist letters. This enables the exchange of these document types using secure messaging[1].

1 *Clinical document types: https://developer.digitalhealth.gov.au/topic/clinical-documents*

# Context for the review

From 2019, state, territory and federal governments agreed to make it a mandatory requirement that secure messaging interoperability standards are referenced in future procurements of all newly implemented digital health technologies. The jurisdictions have also worked with healthcare peak bodies, the clinical software industry and the Australian Digital Health Agency to co-develop FHIR-based interoperability standards and federated directories for secure messaging over the last few years.

Secure Messaging Delivery is a priority area outlined in the National Digital Health Strategy 2018–22 and Framework for Action. The strategy articulates a set of shared outcomes for all stakeholders that complement existing investments in digital health initiatives and that will enable health innovation and improved health and care experiences. Secure messaging is one of the priorities that will facilitate electronic exchange of clinical information between healthcare providers. Interoperability is also seen as a priority which has touchpoints with secure messaging. The seven strategic priorities for digital health in Australia are outlined in Figure 2.

**Figure 2:**
The National Digital Health Strategy seven key strategic priorities

| Strategic Priority | Description |
|---|---|
| My Health Record | Health information will be available whenever and wherever it is needed through the My Health Record. By 2022 all healthcare providers will be able to contribute to and use health information in the My Health Record on behalf of their patients. Patients and consumers will be able to access their health information online or through mobile applications. |
| Secure Messaging **Key Focus** | Healthcare providers will be able to communicate with other professionals via secure digital channels by 2022. Patients will also be able to communicate with their healthcare providers using these digital channels. This will end dependence on paper-based correspondence and fax machine or post. |
| Interoperability and Data Quality **Touch points** | The interoperability of clinical data is essential to high quality, sustainable healthcare – this means that patient data is collected in standard ways and that it can be shared in real time with them and their providers. |
| Medicines Safety | By 2022, there will be digitally enabled paper-free options for all medication management in Australia. People will be able to request their medications online, and all prescribers and pharmacists will have access to electronic prescribing and dispensing, improving the safety of our systems. |
| Enhanced Models of Care **Touch points** | Digital technology can transform outcomes and experiences of different communities in different ways. The strategy proposes a number of pioneering initiatives co-produced between consumers, governments, researchers, providers and industry to test evidence-based digital empowerment of key health priorities, investigate and collectively solve any technical obstacles and then, where appropriate, to promote them nationally. |
| Workforce and Education | The ADHA will collaborate with governments, care providers and partners in workforce education to develop comprehensive proposals so that by 2022 all healthcare professionals have access to resources that will support them in the confident and efficient use of digital services. In addition, the strategy proposes rapid promotion of a network of clinician digital health leaders and champions across Australia. |
| Driving Innovation | The strategy proposes a new initiative to support an expanding set of accredited health apps as well as delivering an improved developer program to enable industry and entrepreneurs to expand existing services and create new ones that meet the changing needs of both patients and providers. |

Secure messaging has the potential to enhance the exchange of clinical information between healthcare providers resulting in safety and quality benefits. Combined with the interoperability paradigm, the wider Australian healthcare sector can expect to benefit from this type of digital information exchange.

The Secure Messaging Program aims to successfully implement secure messaging in the Australian healthcare sector. Currently, the adoption of secure messaging solutions is not where it needs to be and has resulted in pockets of success across Australia. Activities as part of the Agency's Secure Messaging Program are summarised in Table 1.

**Table 1**:
Secure messaging program milestones and related activities – 2017-19

| Milestone | Activity |
|---|---|
| **2017** | — Eliminating paper-based messaging in healthcare approved as a priority of the National Digital Health Strategy 2018–22 |
| **2018** | — Publication of new secure messaging standards and Clinical Document Architecture (CDA) specifications<br>— Two proof of concept secure messaging projects led by two industry consortia (Telstra Health and HealthLink)<br>— Launch of the Agency's digital health test beds program, which includes projects to increase use of secure messaging delivery technology |
| **2019** | — Agency release of an industry offer to promote and accelerate the widespread adoption of secure messaging systems<br>— Service Registration Assistant (SRA) proof of concept to develop a solution for healthcare organisation registration information in external directories<br>— Industry workshop that determined a national scaling approach for secure messaging |

# Scope and methodology

This review examined the safety and quality benefits of secure messaging. These benefits include how 'point-to-point' information sharing via secure messaging can enable enhanced models of care. In addition, this review examined the risk of secure messaging use, including when in operation with parallel adjunct information exchange processes, across a range of clinical environments. Of particular focus were environments that had a greater dependence on manual processes, such as fax, telephone or hand-written information exchange methods.

This review was conducted in four phases to address the scope of the project.

**Figure 3:**

Methodology conducted over four phases

## 01 Desktop and literature review

- Four Agency-provided artefacts were used to understand context, opportunities and barriers of secure messaging
- Twenty papers from the research literature were used to understand the benefits and risks of using secure messaging in healthcare industries across the globe
- Nine Agency stakeholder interviews were conducted to gain further context.

## 02 Clinical scenarios

- Interview guides were developed to align with stakeholder groups and clinical scenarios (referrals, specialist letters, discharge summaries, pharmacy, pathology and diagnostic imaging)
- Key focus was on benefits and risks of using secure messaging, not using secure messaging, barriers and opportunities, functionality for secure messaging to support clinical tasks and cognitive load on clinicians.

**Figure 3** (continued)

**03**

**Stakeholder interviews**

- Twelve stakeholder interviews were conducted across primary care, allied health peak bodies, hospitals and CIS / SMD vendors
- Outputs of the interviews were validated by stakeholders and used to supplement barriers and opportunities from Phase 1, develop key findings, categorise benefits and risk frameworks and develop measures for tracking benefit elements.

**04**

**Final Report**

- Eight recommendations were developed in order to address the key risks and focus on viable opportunities for the secure messaging ecosystem
- Recommendations were made in support of the initiatives outlined in the secure messaging national scaling program
- Exemplar use cases were highlighted and associated success criteria were developed.

# Findings

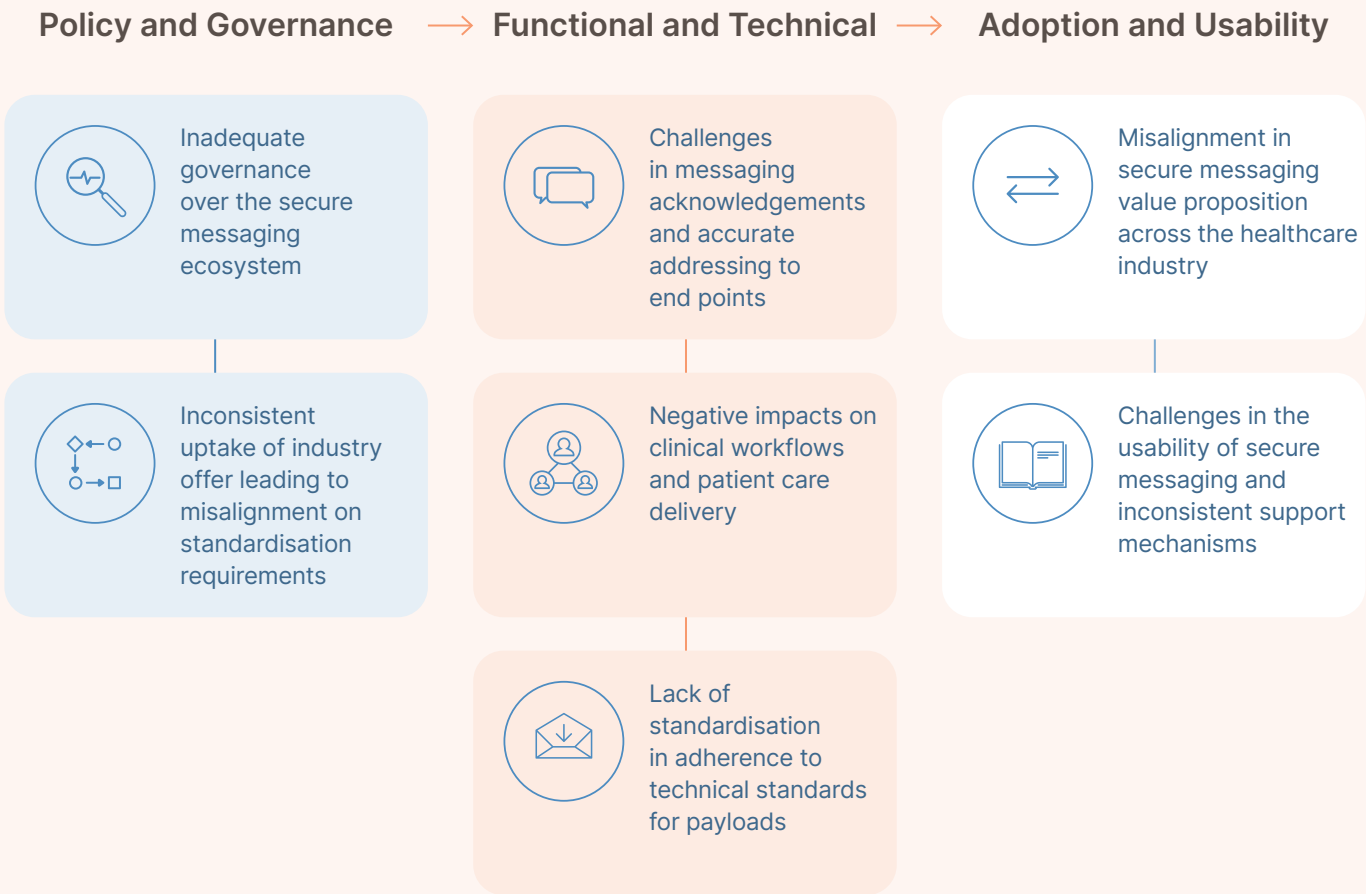
## Barriers to increasing secure messaging adoption

The overarching themes around the barriers to the expansion of secure messaging can be divided into three main categories:

- Policy and governance
- Functional and technical
- Adoption and usability

These barriers (outlined in Figure 4) were sourced from the Secure Messaging for National Scaling report[2] and largely align with the insights gathered from stakeholder interviews in the review.

**Figure 4**:
Key barriers to increasing secure messaging adoption




2 *Australian Digital Health Agency, Deloitte (AU). Secure Messaging National Scaling Final Report. Sydney: ADHA; 2019.*

## Opportunities for increasing secure messaging adoption

There are several Australian Digital Health Agency-led initiatives that are currently under way to progress secure messaging adoption. An industry workshop held in December 2019 between the Agency and the Medical Software Industry Association (MSIA) called for a nationally consistent, standards-based approach to secure messaging, enabling healthcare providers to communicate effectively. This workshop produced the Communique – National Scaling of Secure Clinical Messaging document[3], outlining the agreed national initiatives.

The national scaling initiatives are:

**Initiative 1**
Develop a secure messaging governance framework

**Initiative 2**
Develop secure messaging use cases

**Initiative 3**
Develop standards and a standards framework

**Initiative 4**
Implement a federated directory solution

**Initiative 5**
Develop a trust framework

**Initiative 6**
Support change and adoption across the health sector

**Initiative 7**
Develop a framework of levers.

3 *Communique – National Scaling of Secure Clinical Messaging: Read Here*
*Secure Messaging National Scaling Final Report National scaling report: Read Here*

Additional opportunities and themes for secure messaging were identified during the stakeholder interviews for this review (see Figure 5). These opportunities acknowledge the diverse perspectives of the stakeholders and mostly support the Agency-led initiatives.

**Figure 5**:
Nine opportunities to progress the secure messaging ecosystem identified through the stakeholder consultations in this review

— Establishing a governance framework for the secure messaging environment

— Enhancing seamless clinical information exchange through secure messaging standardisation

— Improving patient data privacy and confidentiality

— Improving the end user experience of secure messaging

— Enabling of clinical workflows and enhanced models of care

— Enhancing of medication mangement workflows

— Supporting patient choice

— Increasing the use of teleheath and remote consultation capabilities due to COVID-19

— Expanding secure messaging to incorporate patient-provider electronic communication

## Benefits of secure messaging

One of the key focus areas of the review was to understand the potential benefit realisation for secure messaging across the Australian healthcare system. While most stakeholder groups interviewed recognise the benefits of secure messaging, these are subject to the healthcare industry collaboratively addressing key secure messaging barriers. It is important to recognise that, while the following benefits are associated with secure messaging, they are also applicable to other digital health technologies.

The benefits of using secure messaging are structured into four key areas – **safety**, **quality**, **efficiency** and **access**. Fifteen benefit elements were mapped from data gathered from the stakeholder interviews, desktop review and the literature review. These benefits are outlined in Figure 6.

**Figure 6:**

Benefits of secure messaging

| Safety | Quality | Efficiency | Access |
|---|---|---|---|
| 1 Improved medication safety | 4 Improved continuity of care | 7 Reduced duplicate testing | 13 Improved data confidentiality and privacy protection |
| 2 Improved patient follow-up after an event or discharge | 5 Improved transfer of care and care coordination | 8 Efficient use of data and information | 14 Improved access to healthcare services |
| 3 Reduced adverse events | 6 Improved patient experience | 9 Improved timelines of information exchange | 15 Access to more complete and accurate clinical information |
| | | 10 Time saved due to effective information transfer | |
| | | 11 Improved end user productivity | |
| | | 12 Improved usability of the CIS and SMD system | |

## Structured data

Structured data is information that can be stored and displayed in a consistent and organised manner. Structured data can be utilised to enrich clinical information exchanges between healthcare information systems and to streamline interoperability across the healthcare industry. For example, a secure message that includes structured data would allow the end system to use all the different data elements from within the message, including clinical information related to pathology results and medications. Conversely, a message that is not structured may only allow the end system to use information in the header of the message such as basic patient information.

Benefits associated with secure messaging can be enhanced through the use of structured data elements. Figure 7 highlights the level of benefit enhancement that can occur in the future by enabling information exchange with structured data elements. Assumptions around each benefit highlighted is supported by data gathered from the interviews and desktop research.

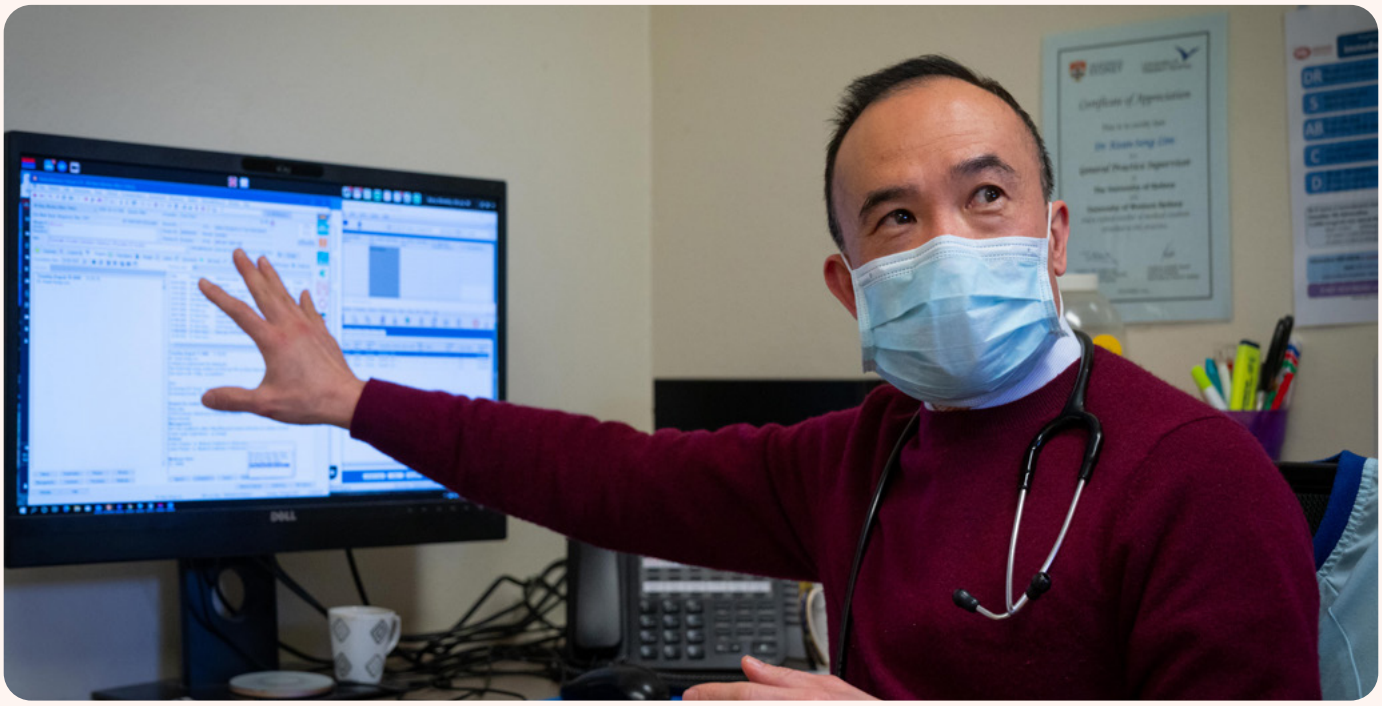


**Figure 7:**

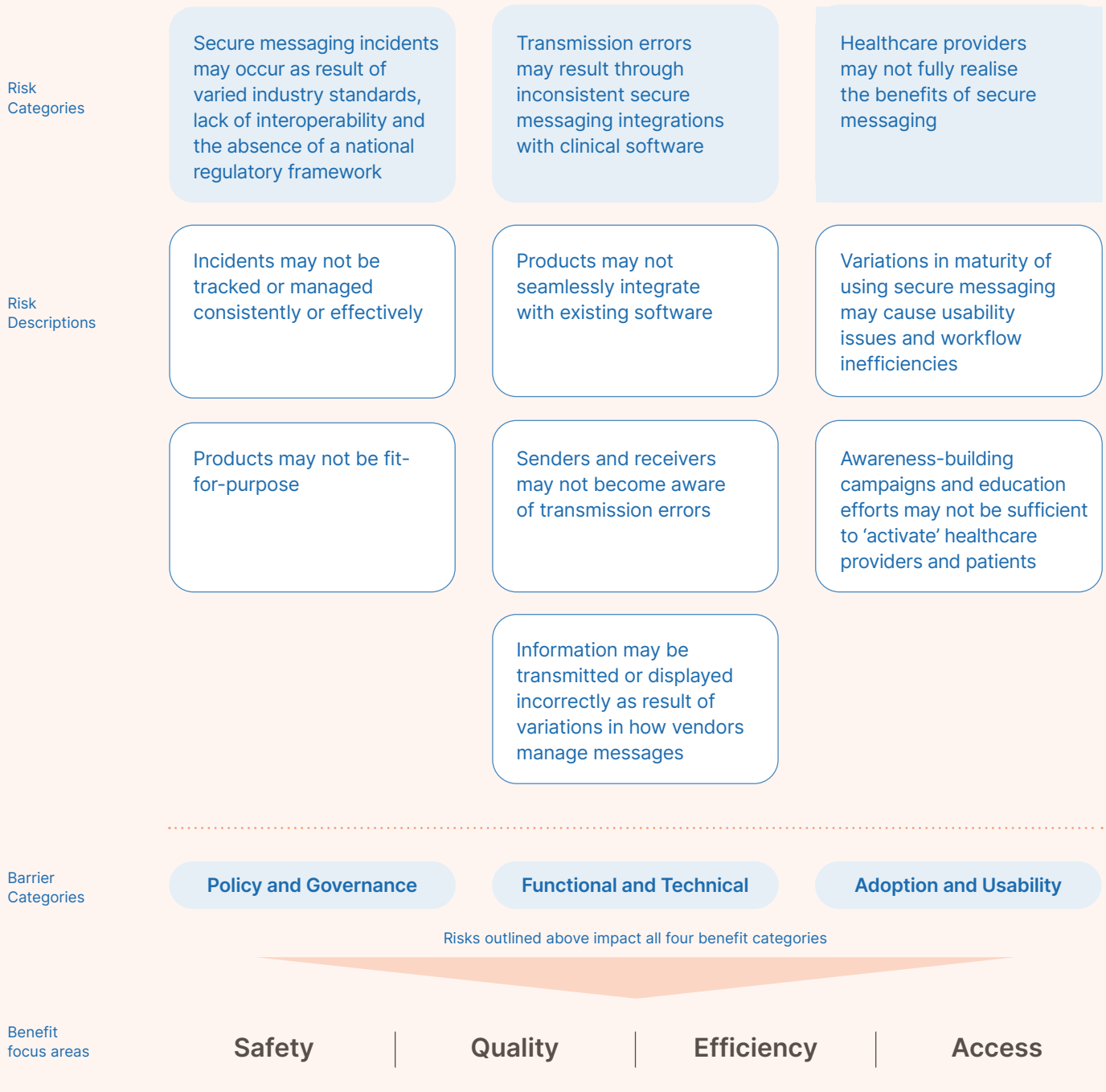
Indicative level of benefit enhancement using structured data elements

## Risks of secure messaging use

Another focus of the review was to understand the risks to safety and quality of care that may arise from secure messaging use. The risks identified through stakeholder interviews are largely caused by the barriers that currently limit system-wide adoption.

The risk categories related to secure messaging use are outlined in Figure 8. These risk categories allow the risks to be mapped to the broader set of barriers that have been identified for secure messaging within the Australian healthcare ecosystem.

**Figure 8:**
Risk categorisation of using secure messaging

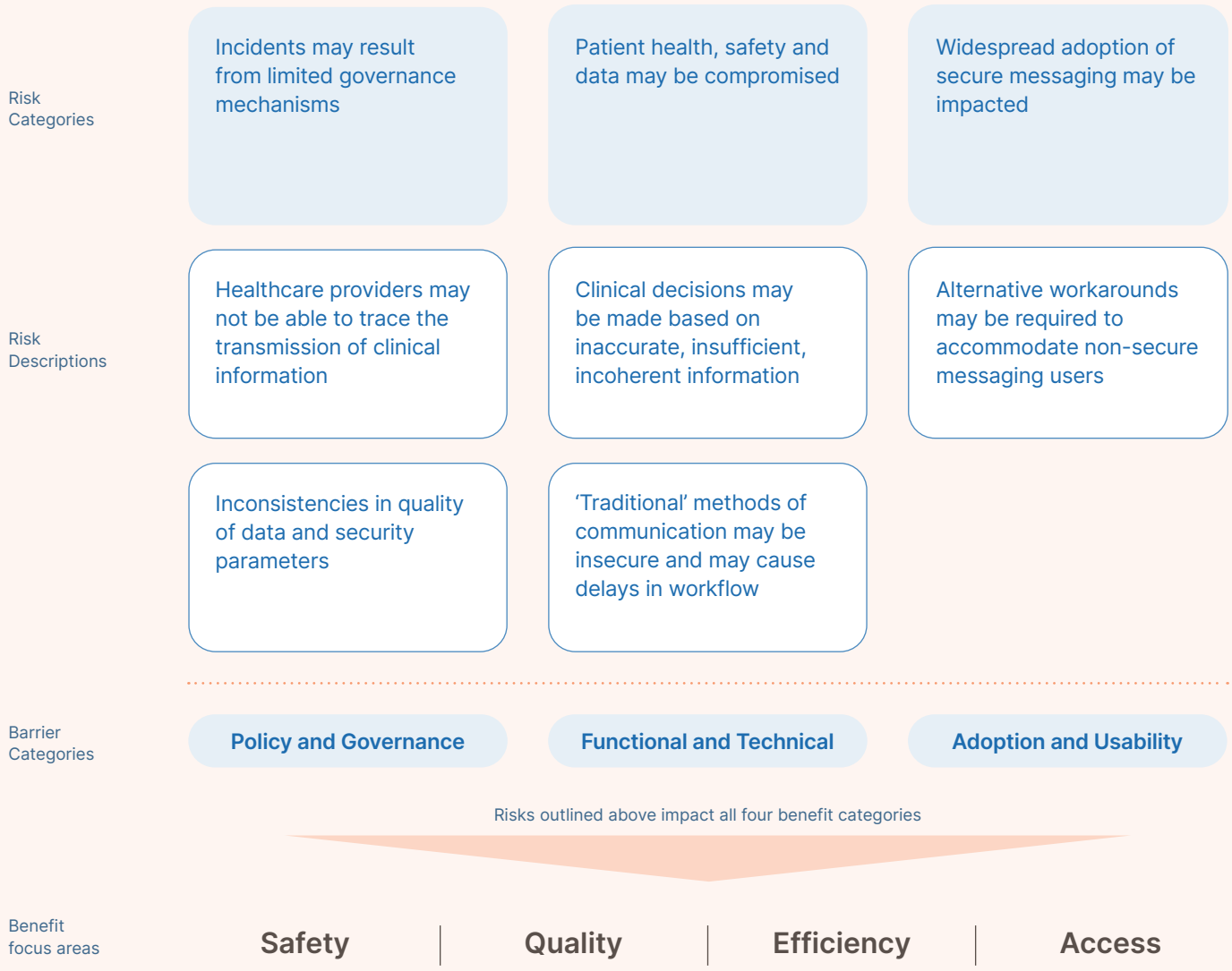


## Risks of not using secure messaging

Another key focus area of the review was to understand the risks to safety and quality of care related to ***not*** using secure messaging. The key risks of not using secure messaging were gathered through the stakeholder interviews, with the consensus view being that the risks of not using secure messaging far outweigh the risks of using secure messaging.

The risks of not using secure messaging are structured into categories outlined in Figure 9. These categories allow the risks to be mapped to the broader set of barriers that have been identified for secure messaging within the Australian healthcare ecosystem.

**Figure 9:**
Risk categorisation of not using secure messaging



# Recommendations

It is important to note that the recommendations of this review support the national scaling initiatives outlined in the 'Communique – National Scaling of Secure Clinical Messaging'. The eight recommendations aim to enhance the safety and quality aspects of secure messaging and enable enhanced models of care. These recommendations support the Agency's national scaling initiatives, which require industry partnerships to ensure their successful implementation.

The eight recommendations of the review (as described in Table 2) are organised into three distinct categories:

- Enable the secure messaging ecosystem
- Enhance the secure messaging capability
- Optimise the current state of secure messaging

**Table 2** (below): Recommendations of the review

| No. | Recommendation |
|---|---|
| Enable the secure messaging ecosystem | |
| 1 | **Identify or leverage existing digital health test beds for evaluating secure messaging for selected use cases and assess user experience**<br>Expanding secure messaging system functionality to support additional use cases is essential to supporting its uptake and increasing adoption across the healthcare sector. Continued evaluation and early adopter testing through the appropriate analysis of healthcare provider networks and potential test beds will enable secure messaging systems and standards. These can be used to enhance clinical workflows within controlled ecosystems, support healthcare provider information exchange and facilitate a patient's choice in provider. |

**Table 2** (continued)

| No. | Recommendation |
|---|---|
| **Enable the secure messaging ecosystem (continued)** | |
| 2 | **Promote the increased use of structured data elements and understand impacts on clinical information capture and exchange**<br>The use of structured data is seen to be one of the key drivers that will uplift secure messaging solution capability and enhance healthcare system interoperability. Secure messaging interoperability requirements need to align with structured data element capabilities which can enhance the benefit focus areas of safety, quality, efficiency and access. |
| 3 | **Consider the development of technical incident monitoring framework to assess adherence to standards**<br>A technical incident monitoring framework should be developed in order to monitor the successful exchanges of secure messages and address transmission errors. Currently, standards for secure messaging have been implemented differently by vendors across the secure messaging ecosystem. Implementation of a framework that supports adherence to clinical documentation standards and secure messaging delivery standards will help to address transmission errors. This monitoring framework will be supported by the governance framework initiative and likely to compel all secure messaging vendors to comply. Note that the current secure messaging industry offer provides a conformance profile that will need to be incorporated into this framework.<br>Furthermore, the use of application level acknowledgement capability will need to be implemented by CIS vendors in order to enable read-receipt functionality. This feature can be used to inform of any incidents that may occur and to enhance clinical workflows by notification of message delivery to the intended end point. |
| **Enhance the secure messaging capability** | |
| 4 | **Assess the impacts of FHIR implementation on the secure messaging ecosystem and understand opportunities to address key barriers**<br>The use of Fast Healthcare Interoperability Resources (FHIR) standards offers a model for clear conformance and test frameworks with secure messaging vendors looking to provide additional support for the FHIR paradigm. It is necessary to understand the impacts of implementing FHIR and the opportunities provided for the Australian secure messaging ecosystem. |

**Table 2** (continued)

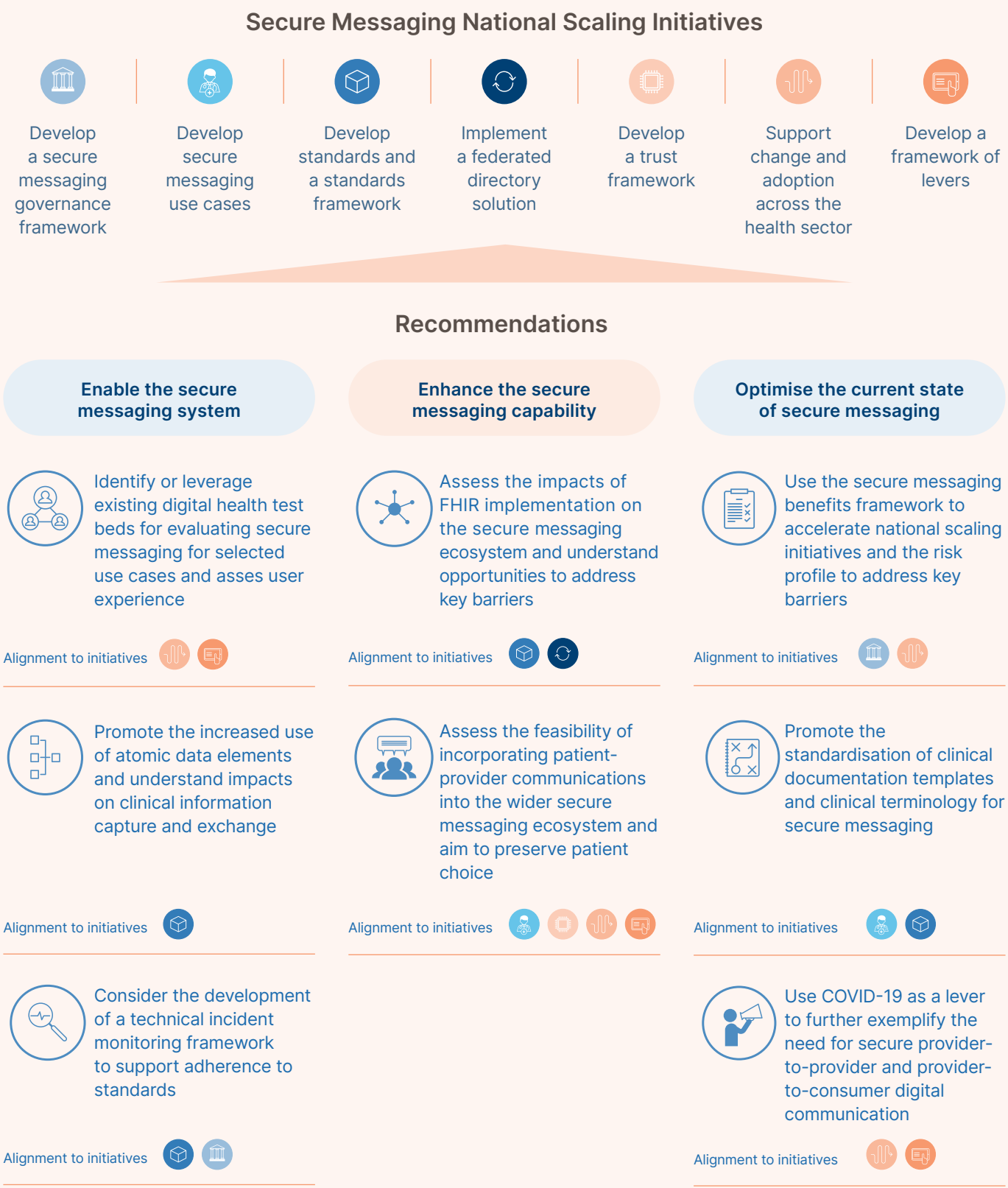
| No. | Recommendation |
|---|---|
| **Enhance the secure messaging capability (continued)** | |
| 5 | **Assess the feasibility of incorporating patient–provider communications into the wider secure messaging ecosystem and aim to preserve a patient's choice**<br>Secure messaging and CIS vendors have started to expand the use of secure messaging to facilitate patient–provider communications and healthcare providers have increased the use of telehealth and remote consultations. The patient–provider communication model can be investigated in order to understand how patient choice in determining their provider can be preserved, and how it can be integrated into secure messaging scope. |
| **Optimise the current state of secure messaging** | |
| 6 | **Use the secure messaging benefits framework to accelerate national scaling initiatives and the risk profile to address key barriers**<br>The benefit focus areas of safety, quality, efficiency and access outlined in the section *Benefits of secure messaging* can be used to accelerate the seven national scaling initiatives detailed in the Communique – National Scaling of Secure Clinical Messaging. These barriers can be addressed by using the risk profile for secure messaging to communicate the implications on safety and quality of care. |
| 7 | **Promote the standardisation of payload specifications relating to clinical documentation templates and clinical terminology for secure messaging**<br>Promoting the standardisation of payload specifications relating to clinical documentation templates for relevant use cases and assessing the use of clinical terminology is necessary to expanding secure messaging adoption and promoting interoperability between secure message information exchange. |

**Table 2** (continued)

| No. | Recommendation |
|---|---|
| Optimise the current state of secure messaging (continued) | |
| 8 | **Use lesson learned from COVID-19 as a lever to further exemplify the need for secure provider-to-provider and provider-to-consumer digital communication**<br>Changes driven by social distancing have accelerated the need to roll out and adopt digital healthcare models and tools. Out of necessity, there has been a shift in provider and consumer attitudes with regard to engaging in and receiving forms of healthcare virtually. This can be used as a lever to demonstrate the benefits of secure messaging. Peak bodies and primary health networks can play an important role in building awareness, promoting advocacy and upskilling the workforce around the need for secure forms of digital communication. |

These recommendations and their alignment to the national scaling initiatives in the Communique are outlined in Figure 10.

**Figure 10:**
Alignment of recommendations to National Scaling Initiatives



# Key success criteria

Based on the desktop review and inputs from stakeholder interviews, several success criteria were identified to support the national scaling of secure messaging across Australia's health sector. These criteria largely align with those proposed as part of the ***Secure Messaging National Scaling Final Report 2019***.

## Whole-of-sector approach

Critical to the national scaling of secure messaging is the need for a concerted approach to secure messaging roll-out and adoption. Secure messaging benefit realisation can be maximised through a whole-of-sector approach that promotes collective learning and a streamlined method of communication and information exchange.

## Promoting interoperability

Interoperability between clinical information systems and secure messaging systems across the sector allows for an integrated, seamless and unified end user experience which is critical for any national scaling efforts.

## Sound governance mechanisms

Clear transparency, ownership, and incident management requirements are key to successfully scaling and sustaining secure messaging. Governance is critical to enabling other key success criteria for driving the national scaling of secure messaging.

## Adherence to standards

Adherence to agreed standards that are tailored to use cases can facilitate the clinical information exchange. To enable this, standards need to be articulated clearly to promote consistent interpretation and application across the sector.

## Data accuracy and consolidation

It is important to encourage data completeness and quality across healthcare provider directories to avoid data duplication and enhance secure messaging capabilities.

## Ensuring privacy and security

Healthcare provider communication via secure messaging vendors should incorporate secure and trusted message exchange mechanisms that protect sensitive patient information.

## Putting users at the centre

Provide a consistent, accessible and frictionless user experience to enable broad secure messaging adoption for end users. Enhancing user experience is dependent on achieving the aforementioned success criteria, as well as ensuring continuous feedback is achieved to support system design and implementation.

## Pragmatic initiatives

The use cases outlined and ranked in the review demonstrate whether initiatives will enable quick wins and effectively address the key challenges in the secure messaging ecosystem.

# Conclusion

This review has found widespread recognition of the potential benefits of secure messaging across the stakeholders interviewed; however, low uptake as a result of barriers and perceived risks to patient safety and quality will continue to challenge uptake and broader adoption.

The barriers and risks raised throughout the stakeholder interviews led to the identification of opportunities to address gaps in the current secure messaging ecosystem. The increased rate of digital adoption through the COVID-19 pandemic provides one of the major opportunities for acceleration in digital health transformation initiatives worldwide. These opportunities enable the realisation of secure messaging benefits across safety, quality, efficiency and access and incorporate specific use cases where secure messaging or other digital solutions have demonstrated reasonable success. These opportunities also reflect the diverse views of stakeholders interviewed, providing insight into stakeholder priorities and the attitudes prevalent across the sector.

To enable the fulfilment of these opportunities and the mitigation of the risks identified with the use of secure messaging, several recommendations were outlined in the review that align to the Communique – National Scaling of Secure Clinical Messaging as well as the National Digital Health Strategy 2018-22 and the associated Framework for Action. This was supplemented by several success criteria that can enable the future state of secure messaging.

Australian Government

Australian Digital Health Agency

AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE