



Australian Government
Australian Digital Health Agency

Secure Messaging National Scaling Final Report

Table of Contents

Section	Slide number
List of Abbreviations and Acronyms	3 - 3
Executive Summary	4 - 5
Introduction	6 - 15
Current State	16 – 28
Global Scan	29 – 34
Future State	35 – 38
Gap Analysis	39 - 45
Initiatives	46 - 80
Governance Framework	81 - 97
Roadmap	98 - 105
Recommended Next Steps	106 – 107
Appendix	108 - 113



List of Abbreviations and Acronyms

ADHA	Australian Digital Health Agency	MSIA	Medical Software Industry Association
AHMAC	Australian Health Ministers' Advisory Council	MU	Meaningful Use
AMA	Australian Medical Association	NASH	National Authentication Service for Health
API	Application Programming Interface	NDHS	National Digital Health Strategy
CDA	Clinical Document Architecture	NHIR	National Health Interoperability Roadmap
CEHRT	Certified Electronic Health Records Technology	NHS	National Health Service
CHC	COAG Health Council	NRC	National Release Centre
CIS	Clinical Information Systems	NSQHS	National Safety and Quality Health Service
CMS	Centers for Medicare & Medicaid Services	PHN	Primary Health Network
COAG	Council of Australian Governments	PKI	Public Key Infrastructure
CSIRO	Commonwealth Scientific and Industrial Research Organisation	PMS	Practice Management System
DIAS	Diagnostic Imaging Accreditation Scheme	RACGP	Royal Australian College of General Practitioners
DoH	Department of Health	RACS	Royal Australasian College of Surgeons
EMR	Electronic Medical Record	SMD	Secure Messaging Delivery
ePiP	Practice Incentives Program eHealth Incentive	SRA	Service Registration Assistant
FHIR	Fast Healthcare Interoperability Resources	UX	User Experience
GP	General Practitioner		
GUI	Graphical User Interface		
HL7	Health Level 7		
HSO	Health Standards Organisation		
KPI	Key Performance Indicator		



Case for Change | The success of the Secure Messaging Program plays an imperative role in achieving the Australian National Digital Health Strategy's key priorities for 2022

Why change?

Currently, a large percentage of healthcare organisations and practitioners (those with and without a Secure Messaging solution) revert to using manual, paper-based transactions and/or fax. This imposes risk on:



Transfer of care, the printing of referral letters and other clinical documents shift responsibility to the patient to pass information to the next healthcare provider



Patient data confidentiality, as manual workflows, e.g. paper-based transactions and fax, are not meeting patient data confidentiality requirements



Data quality and integrity, as administrators manually upload data to digital records, thus introducing the risk of transcription error

Manual transactions hinder the quality of patient care and clinical safety

Why change now?

The Australian National Digital Health Strategy (2019 – 2022) has 7 key strategic priorities:

- 1 Health information that is available whenever and wherever it is needed
- 2 Health information that can be exchanged securely
- 3 High-quality data with a commonly understood meaning that can be used with confidence
- 4 Better availability and access to prescriptions and medicines information
- 5 Digitally-enabled models of care that improve accessibility, quality, safety and efficiency
- 6 A workforce confidently using digital health technologies to deliver health and care
- 7 A thriving digital health industry delivering world class innovation

Why focus on Secure Messaging?

Strategic priority 2 speaks directly to Secure Messaging. Secure Messaging is more efficient and timely and leverages existing digital processes (such as EMR or CIS). It has multiple benefits that directly or inherently support the vision of the National Digital Health Strategy (2022):

- Secure exchange of clinical information **prevents unauthorised interception** of the message content
- **Reduced** use of **paper** correspondence
- **Confidential patient correspondence** only seen by treating clinicians
- System notification of message delivery, so that sending organisations **know** that **messages** have been **received**
- Potential to **improve** the **timeliness** of receipt of clinical information, and therefore the **quality of care** provided
- Over time as software vendors enhance their digital health functionality, **consolidation of information** in clinical software can be achieved

Better health for all Australians enabled by seamless, safe, secure digital health services and technologies that provide a range of innovative, easy to use tools for both patients and providers

Sources

1. National Digital Health Strategy (<https://conversation.digitalhealth.gov.au/>)
2. ADHA website (<https://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/secure-messaging>)



Executive Summary | Secure Messaging National Scaling and Associated Roadmap

The **Agency** has **appointed Deloitte** to assist in **identifying** the **barriers** to the adoption of Secure Messaging. The consultation and feedback through stakeholder interviews and workshops has enabled Deloitte to develop a **Secure Messaging National Scaling** and an associated **roadmap**. The roadmap depicts a **pragmatic** and **realistic** list of initiatives that will assist in progressing adoption. The engagement commenced 22 July 2019 and is scheduled to be completed 4 October 2019.

What we did

The approach taken for the development of the Secure Messaging National Scaling and roadmap included stakeholder engagement, analysis and validation activities.

Kick Off and Mobilise

Kick off and mobilisation activities included facilitating a kick off session where engagement activities, timelines and the stakeholder list for consultation were confirmed. A document review was also undertaken.

Stakeholder Engagement

Stakeholder engagement activities included conducting one-on-one interviews, group workshops and an external survey. The one-on-one interviews and group workshops targeted internal ADHA and vendor stakeholders, while the external survey targeted end users.

Current State Analysis

Analysis of the current state was guided by user-centred design principles. Team analysis was conducted to gather, collate, categorise and analyse data. Key themes were subsequently validated with internal and external stakeholders.

Initiative and Roadmap Development

Based on the challenges identified in the Current State, key initiatives were identified and prioritised to form the Secure Messaging National Scaling roadmap.

What we saw

Based on our engagement with ADHA, vendors, healthcare jurisdictions, thought leaders and end users, we identified a number of themes and challenges across the Secure Messaging Ecosystem currently impacting adoption.

The Ecosystem and Challenges



The challenges identified were specific to five key areas of the Secure Messaging Ecosystem, namely Governance, Industry, Technical Capability, End User and Clinical Safety and Quality.

Personas

Eight primary end user personas were identified:

- | | |
|----------------------|---------------------------|
| General Practitioner | Imaging |
| Specialists | Allied Health |
| Hospitals | Pharmacists |
| Pathologists | Other Healthcare Services |

What we recommended

Eight guiding principles were designed to support the development of the future state:

- Data accuracy & consolidation
- Whole of sector approach
- Ensuring privacy and security
- Pragmatic initiatives
- Putting users at the center
- Promote interoperability
- Adherence to standards
- Sound governance

Initiatives and Roadmap

Eight key initiatives were identified to accelerate adoption, of which seven are culminated into a three staged, pragmatic roadmap:

- | | |
|--|--|
| Develop a Secure Messaging Governance Framework | Review NASH Processes and Develop a Suitable Trust Framework (<i>in progress</i>) |
| Develop Secure Messaging Use Cases | Establish a Change and Adoption Program |
| Agree on Secure Messaging Standards & Develop a Standards Framework (<i>in progress</i>) | Develop a Secure Messaging Lever Framework |
| Implement a Federated Secure Messaging Directory Solution (<i>in progress</i>) | Establish an Innovation and Research Function (<i>Addressed by wider NDHS / NHIR initiative</i>) |



Introduction

Introduction

Current State

Global Scan

Future State

Gap Analysis

Initiatives

Governance
Framework

Roadmap

Recommended
Next Steps

Appendix



Why we are here: To develop a **Secure Messaging National Scaling** and associated **roadmap**, which is **pragmatic** and **achievable** whilst recognising the complexities that exist within the current system



Secure Messaging is a core foundational capability required to enable interoperable, safe, seamless, secure, and confidential information sharing across all healthcare providers and consumers. Reliable, secure provider-to-provider communication is a key component of digitally enabled, integrated and coordinated care across the Australian healthcare sector.



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.



The **Agency appointed Deloitte** to assist in **identifying** the **barriers** to the adoption of Secure Messaging. Through various stakeholder interviews and workshops, Deloitte developed a **Secure Messaging National Scaling** and associated **roadmap**. The roadmap depicts a **pragmatic** and **realistic** list of initiatives that will assist in progressing adoption. The engagement commenced 22 July 2019 and is scheduled for completion on the 4th October 2019.



The National Digital Health Strategy outlines four key themes which summarise what Australia wants from digital health

Support me in making the right healthcare choices, and provide me with options - Patient

Clinicians, healthcare providers and Peak bodies see the benefits of patient empowerment and access to information but recognise that reduced access to the internet among some socio-economic and demographic groups poses risks to healthcare access and equity that need to be addressed. They believe it is critical that patients are not left behind through the increased reliance upon digital health technologies and services.



Help all the people who care for me to understand me, and together, provide safe and personalised care - Patient

In order to facilitate this, clinicians and healthcare providers need to have trust and confidence in the accuracy and completeness of their patients' information, allowing them to deliver the right health advice to patients, which will lead to better outcomes. Clinicians and healthcare providers are willing to use digital technology, but require evidence showing the value of such technology before investing in change to their current working practices. Clinicians and healthcare providers recognise the need to move from providing undifferentiated care to increasingly personalised care, and realise the reliance that this approach will have upon strong digital health foundations.

Create an environment where my healthcare providers and I can use and benefit from innovative technologies - Patient

To support these expectations, clinicians and healthcare providers need ongoing training, as well as high-quality and reliable digital health technology, clinical information systems and internet connections, to ensure that they are able to use digital health technology and services effectively.



Preserve my trust in the healthcare system and protect my rights - Patient

Clinicians and healthcare providers need greater confidence in the security of the systems that enable them to share patient information with other clinicians. They need assurance that the digital systems they use support them to meet their obligations to keep their patients' health information secure and private, and that health data will be used safely and appropriately to improve patient outcomes.

Sources








1. National Digital Health Strategy (<https://conversation.digitalhealth.gov.au/>)



The National Digital Health Strategy defines seven key strategic priorities to be achieved by 2022. Secure Messaging Adoption is one of the priorities and the focus of this engagement

The National Digital Health Strategy articulates a set of shared outcomes for all stakeholders that complement existing investments in digital health initiatives and will enable health innovation and improved health and care experiences to be delivered.

The seven strategic priorities for digital health in Australia are as follows:

 Availability	 Secure Messaging	 Interoperable	 Medicines Safety	 Enhanced Models of Care	 Educated	 Innovative
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.	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 the fax machine or post.	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.	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.	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.	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.	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.
	Key Focus	Touchpoints				

Sources

1. National Digital Health Strategy (<https://conversation.digitalhealth.gov.au/>)



Our user-centric approach to developing the Securing Messaging National Scaling is underpinned by five key design principles



Fundamentally user-centered

To develop a strategy or solution that is impactful, usable and desirable, we must put the users at the heart of the approach and involve them deeply in the process as co-creators.



Fit for purpose research techniques

We will leverage relevant research techniques to gain the appropriate depth and insight into the needs, challenges and preferences of your stakeholder groups.



Agile and iterative

Throughout the process our team is committed to continually learning and evolving our approach, as new insights surface. To maximise insights drawn from the design process, we believe in adopting a continuous feedback loop.



Co-design and collaboration

We will work collaboratively with you and your customer groups through a series of co-design workshops and working group sessions. Together, we will ideate, develop concepts, then test and refine these into an innovative and intuitive output that is valuable.



Design with the end in mind

In addition to working towards a design being impactful to the users, it also needs to be economically viable, and technically and culturally feasible.

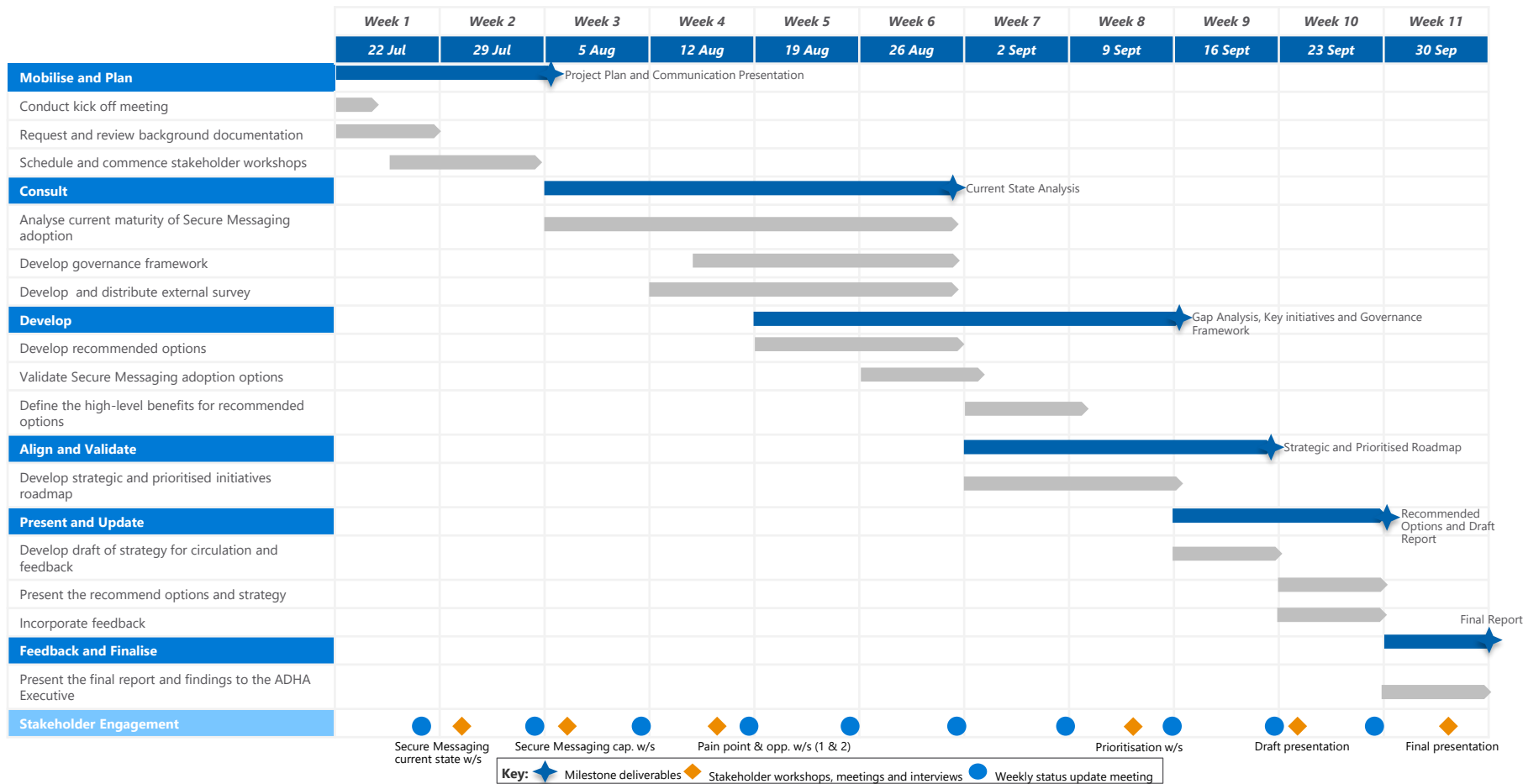


A detailed approach enabled us to work with you to quickly and iteratively define, analyse and refine our recommendations

	Week 1 - 2 (22 July – 2 August)	Week 3 - 5 (5 – 23 August)	Week 5 - 6 (19 – 30 August)	Week 7 - 8 (2 – 13 September)	Week 9 - 10 (16 – 27 September)	Week 11 (30 September – 4 October)
Deliverable	Project Plan and Communication Presentation	Current State Analysis	Gap Analysis, Key initiatives and Governance Framework	Strategic and Prioritised Roadmap	Recommended Options and Draft Report	Final Report
	Mobilise and Plan	Consult	Develop	Align and Validate	Present and Update	Feedback and Finalise
Goal	Kick off project, commence document review and stakeholder consultation	Analyse the current state and draft governance framework	Develop prioritisation and strategic roadmaps	Finalise and validate recommended options	Present the recommended options and strategy	Receive and incorporate feedback. Present the agreed strategy to the Executive
Detailed Activities	<ul style="list-style-type: none"> Kick off meeting Confirm project team, stakeholders and meeting Confirm objectives and approach Request and review background documentation Finalise project plan and accountabilities Schedule stakeholder meetings/interviews or workshops Commence stakeholder consultation and workshops 	<ul style="list-style-type: none"> Analyse current maturity of Secure Messaging adoption Continue stakeholder consultation and workshops Develop recommended options for Secure Messaging adoption Develop governance framework Develop and distribute the external survey 	<ul style="list-style-type: none"> Continue stakeholder consultation and workshops Validate Secure Messaging adoption options Define the high-level benefits for recommended options 	<ul style="list-style-type: none"> Continue stakeholder consultation and workshops Develop strategic and prioritised initiatives roadmap 	<ul style="list-style-type: none"> Develop presentation and draft of strategy for circulation and feedback Present the recommend options and strategy Incorporate initial feedback from the meeting 	<ul style="list-style-type: none"> Gather and incorporate final feedback into the final version of the report Present the final report and findings to the ADHA Executive
Outputs	<ul style="list-style-type: none"> High-level presentation for Executive communication Project Plan Stakeholder meetings and interviews scheduled Current State Workshop and Assessment Stakeholder Map 	<ul style="list-style-type: none"> Identified preferred options for Secure Messaging adoption Governance framework External stakeholder survey Pain Points & Opportunities Workshops 	<ul style="list-style-type: none"> Secure Messaging adoption options finalised Benefits for recommended options proposed 	<ul style="list-style-type: none"> Prioritisation Workshop Strategic and prioritised roadmap 	<ul style="list-style-type: none"> Draft report including recommended options, proposed strategy and associated roadmap 	<ul style="list-style-type: none"> Final report



The engagement spanned over 11 weeks, which included mobilisation, consultation, analysis, development and validation activities



Our consultations included both one-on-one interviews and collaborative workshops

1	2	3	4	5	6
Current State Workshop	1:1 Interviews	Pain Points & Opportunities Workshop	Prioritisation Workshop	Draft Presentation	Final Presentation
<ul style="list-style-type: none"> Identify healthcare agencies and supporting services who depend on clinical correspondence. Touch on capabilities Identify and discuss vendor perspectives Identify challenges within the ecosystem Discuss vision and future state Identify opportunities for improvement 	<ul style="list-style-type: none"> Ascertain the ADHA executives individual perspective on the vision, current pain points, opportunities and outstanding queries Recognise Secure Messaging development efforts to date and how ADHA could drive the optimisation of those capabilities Ascertain external stakeholder perspective on the vision, current pain points and opportunities 	<ul style="list-style-type: none"> Determine the Secure Messaging adoption challenges Workshop with the CIS vendors Workshop with SMD vendors 	<ul style="list-style-type: none"> Validate and prioritise the identified Secure Messaging Adoption initiatives 	<ul style="list-style-type: none"> Present the draft report of strategy and associated roadmap to ADHA Executives 	<ul style="list-style-type: none"> Present the final report of strategy and associated roadmap to ADHA Executives (with feedback incorporated from the draft presentation)
08/08	09/08 to 09/09	15/08	12/09	23/09	01/10
ADHA Stakeholders	ADHA Internal and External Stakeholders	CIS and SMD vendors	ADHA Stakeholders	ADHA Stakeholders	ADHA Stakeholders

Five key groups of stakeholders were engaged throughout the consultation



End Users

The end users of the Secure Messaging process interact with Secure Messaging via multiple end points:

- Primary healthcare – Can be a patient's first point of contact to get care and includes General Practice, Allied Health Services, Pharmacy and Community Health
- Primary Health Networks – Play a coordinating and supporting role for healthcare providers
- Hospitals – Deliver a range of services to patients
- Specialists – Generally referred to by Primary Health Care Providers
- Other – non-healthcare providers and supporting bodies



Internal ADHA Stakeholders

As part of their role at the Agency these people provide overarching vision and direction for Secure Messaging adoption:

- Executives
- Program Delivery Leads
- Senior Clinical Reference Lead
- Board Members / Advisors / Medical Directors and Presidents of Associations
- Product Managers
- Directors – Innovation, Implementation & Support Services
- General Manager for Partnerships and Clinical Use



External Stakeholders

External stakeholders (excluding CIS and SMD vendors) who play an independent and advisory role:

- CSIRO – Provide an independent perspective on the future of emerging healthcare technologies
- Peak bodies (RACGP, MSIA, etc.) – Are the representative voice of members in the discussion and negotiations with Government
- Secure Messaging industry specialists – stakeholders who have provided research and insights into Secure Messaging technical standards and processes
- Health jurisdictions



Secure Messaging Delivery (SMD) Vendors

SMD vendors service end users and collaborate with CIS vendors to support the transfer of electronic clinical information between CIS solutions:

- Multiple SMD vendors provide services across Australia



Clinical Information System (CIS) Vendors

CIS or Practice Management System (PMS) vendors service end users and digitally enable healthcare providers:

- Provides systems that enable clinicians to make informed decisions about patient care
- Multiple CIS vendors provide services across Australia



Personas that describe the unique characteristics and behaviours of primary end users were identified

Understanding the way people work tells us how they need to interact with the Secure Messaging process and use it to enable patient-centric outcomes.



General Practitioner

A general practitioner (GP) is a doctor who is also qualified in general medical practice. GPs are often the first point of contact for someone, of any age, who feels sick or has a health concern. They treat a wide range of medical conditions and health issues¹.



Specialists

Specialists are doctors who have completed advanced education and training in a specific area of medicine. You usually need a letter of referral from your general practitioner (GP) to make an appointment to see a Specialist¹.



Hospitals

Hospitals deliver a range of services to admitted and non-admitted patients (outpatient clinics and emergency department care). State and territory governments largely own and manage public hospitals—which usually provide ‘acute care’ for short periods. Private hospitals are mainly owned and operated by either for-profit companies or not-for-profit organisations; they can include day hospitals as well as hospitals providing overnight care².



Pathologists

Pathologists are specialist medical practitioners who study the cause of disease and the ways in which diseases affect our bodies by examining changes in the tissues, in blood and other body fluids³.



Imaging

Medical imaging encompasses different imaging modalities and processes to image the human body for diagnostic and treatment purposes. Medical imaging includes the engagement of a multi-disciplinary team which include radiologists, radiographers, sonographers, medical physicists, nurses and biomedical engineers⁴.



Allied Health

Allied health professionals are health professionals that are not part of the medical, dental or nursing professions. These types of practitioners often work within a multidisciplinary health team to provide specialised support for different patient needs⁵.



Pharmacists

Pharmacists work in community pharmacies, hospitals, pharmaceutical production on sales or in primary care organisations. Pharmacists are responsible for the quality of medicines supplied to the patients, ensuring that the supply of medicines is within lawful use, making sure prescribed medicines are suitable to the patients and advising patients about medicines⁶.



Other Service Providers

Encompasses all other support services a patient accesses and associated services including community care providers (e.g. Meals on wheels)

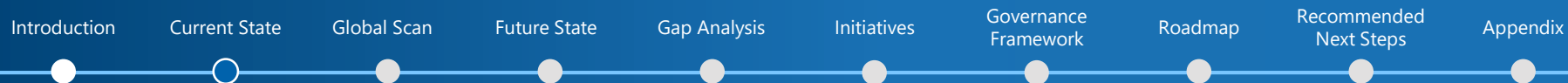
Sources

1. BetterHealth Channel (<https://www.betterhealth.vic.gov.au/health/serviceprofiles/General-practitioner-services>)
2. Australia's health 2018, Australia Institute of Health and Welfare
3. The Royal College of Pathologist of Australia <https://www.rcpa.edu.au/Pathology-Careers/What-is-Pathology>

4. Diagnostic Imaging (https://www.who.int/diagnostic_imaging/en/)
5. Allied Health Professions Australia <https://ahpa.com.au/what-is-allied-health/>
6. General Pharmaceutical Council – What does a pharmacist do? (<https://www.pharmacyregulation.org/raising-concerns/raising-concerns-about-pharmacy-professional/what-expect-your-pharmacy/what-does-0>)



Current State



The analysis of the Current State consisted of five key activities that were performed in order to understand the challenges across the Secure Messaging Ecosystem



Document Review

Documents, research reports and whitepapers were reviewed to gain context from internal and external perspectives.



Workshops

A series of current state, pain points and opportunities workshops were conducted with both internal and external stakeholders.



Interviews

Interviews were conducted with internal ADHA stakeholders, multiple Clinical Information System (CIS) vendors, Secure Messaging Delivery (SMD) vendors, emerging technology thought leaders and jurisdictional health departments.



External Survey

An external survey was distributed and used to understand end user challenges and opportunities with regards to Secure Messaging.



Team Analysis and Validation

Guided by user-centred design principles, team analysis was conducted to gather, collate, categorise and analyse data. Key themes were subsequently validated with internal and external stakeholders.



Four workshops were conducted in order to understand the current state Secure Messaging challenges, identify opportunities for improvement and prioritise initiatives

Current State Workshop

Purpose: An internal workshop with ADHA stakeholders to identify and validate the current state end user and vendor challenges and identify opportunities for adoption of Secure Messaging.

The current state workshop incorporated the following activities:

1. **Identify** healthcare agencies and supporting services who can utilise Secure Messaging and rate their digital maturity
2. **Identify** the vendor touchpoints with regards to Secure Messaging
3. **Discuss** current Secure Messaging capabilities
4. **Understand** where the challenges are in the current end-to-end Secure Messaging process
5. **Discuss** vision and future state
6. **Identify** opportunities for improvements in adoption in the short term (1-3 years) and long term (beyond 3 years)

Pain Points and Opportunities Workshop (x2)

Purpose: An external workshop with vendors to understand the current state challenges for CIS and SMD vendors and identify opportunities for adoption of Secure Messaging.

The two pain point and opportunities workshops with the CIS and SMD vendors covered the following activities:

1. **Identify** example Use Cases and discuss end user perspectives
2. **Validate** high level Secure Messaging capability and CIS provider involvement
3. **Identify** and explore areas where Secure Messaging is working well
4. **Understand** the current challenges in the Secure Messaging process
5. **Identify** opportunities for improvements in adoption in the short term (1-3 years) and long term (beyond 3 years)

Prioritisation Workshop

Purpose: Validate and prioritise the identified Secure Messaging Adoption initiatives.

The prioritisation workshop covered the following activities:

1. **Recap** of themes identified during the current state analysis
2. **Review, validate and prioritise** proposed initiatives
3. **Explore** and discuss additional initiatives



An external survey was distributed and used to understand end user challenges and opportunities with regards to Secure Messaging

The following questions were included in the external survey. The structure of the survey allowed us to differentiate between those who currently used a Secure Messaging solution, those who had a Secure Messaging solution implemented but did not use it, and those who did not have a Secure Messaging solution implemented at all.



Purpose – To obtain healthcare provider details including location, role and additional statistics

1. Where do you work in Australia?
2. What type of practitioner or healthcare provider are you?
3. What is your job role?
4. On average, how many discharge summaries, specialist letters and referrals do you receive per day?
5. On average, how many discharge summaries, specialist letters and referrals do you receive electronically (i.e. email, digital fax or system) per day?
6. On average, how many discharge summaries, specialist letters and referrals do you send per day?
7. On average, how many discharge summaries, specialist letters and referrals do you send electronically (i.e. email, digital fax or system) per day?
8. How many patients are you servicing per day?
9. Do you have a Secure Messaging solution implemented? (Note that this does not include encrypted email or digital fax)



Purpose – To understand who has implemented a Secure Messaging system solution

10. What clinical or practice management system(s) do you use most often for Secure Messaging?
11. What messaging agent(s) do you use most often for Secure Messaging?
12. How often would you use Secure Messaging?

Purpose – To understand who has implemented a Secure Messaging solution but do not use it as often

13. What are some of the challenges that limit you from using Secure Messaging more often?
14. Please share any suggestions on how the process or technology can be improved to increase adoption of Secure Messaging

Purpose – To understand some of the benefits realised for those who use Secure Message often

15. What are some of the benefits you have recognised by using Secure Messaging?
16. What's working well for you by using Secure Messaging?
17. Please share any suggestions on how the process / technology can be improved to increase adoption of Secure Messaging



Purpose – To understand why Secure Messaging is not implemented

18. Why have you not implemented Secure Messaging?
19. How do you currently send referrals, discharge summaries or specialist letters to another healthcare provider?
20. What do you believe are the benefits of digitising your process?
21. If you were to digitise your process, what would be your specific requirements?
22. Please share further suggestions on how you would like to reduce paper-based communication?



Introduction Current State Global Scan Future State Gap Analysis Initiatives Governance Framework Roadmap Recommended Next Steps Appendix

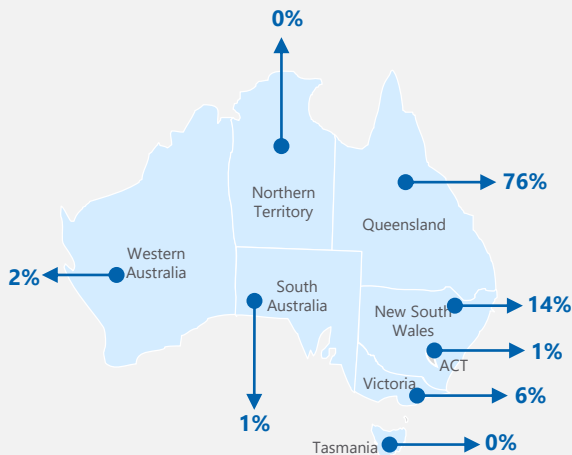
The survey responses provided a unique end user perspective that has been incorporated into the current state analysis (1/2)

Number of Responses

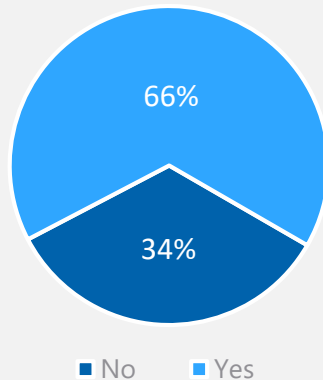
88

Responses

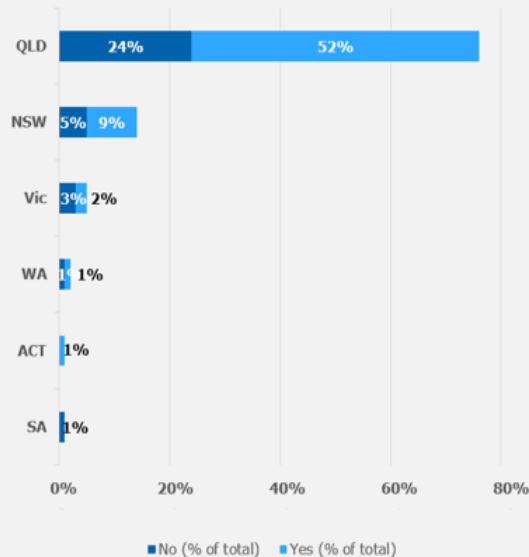
Location of Respondents



% of Respondents who have a Secure Messaging solution implemented

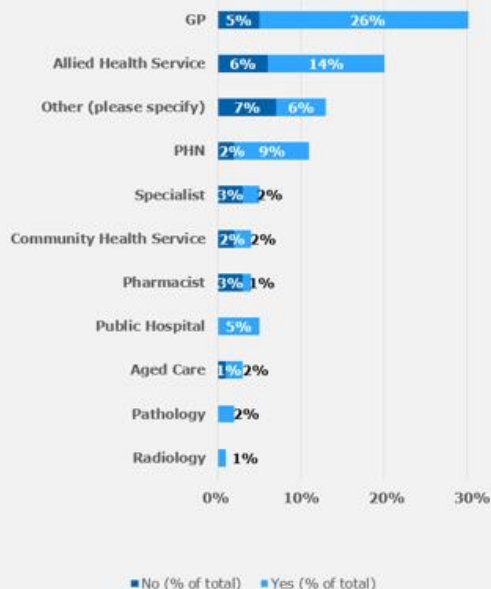


% of Respondents who have a Secure Messaging solution implemented by location

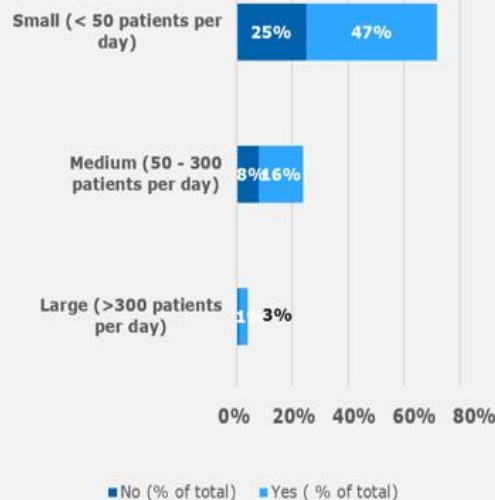


The survey responses provided a unique end user perspective that has been incorporated into the current state analysis (2/2)

% of Respondents who have a Secure Messaging solution implemented by provider type



% of Respondents who have a Secure Messaging solution implemented by the number of patients serviced per day



Other key takeaways

For end users who had a Secure Messaging solution:

- Some common clinical or practice management systems that were used were Best Practice, Medical Director, Coreplus, Healthkit, Zedmed and Helix
- Some common SMD vendors used were Medical Objects, Argus, ReferralNet and HealthLink
- Some providers who had a Secure Messaging solution installed, did not use it as often as they did not receive much correspondence through their clinical or practice management systems

For end users who did not have a Secure Messaging solution, some key takeaways are listed below:

- Some end users did not invest in a solution as they did not see the value in the current Secure Messaging solution
- There are some hospitals that are not digitally mature. Fax machines are still used for the exchange of clinical information
- End users wanted a GUI / UX / interface that was easy to use and consistent across all platforms, secure access to confidential information and wanted integration to other applications such as Healthkit
- End users within certain regions reported that other healthcare providers they regularly communicated with did not use Secure Messaging. Email, fax, post and printing was used to communicate with those providers



Of the 66% respondents who had a Secure Messaging solution implemented, many have given feedback on opportunities to improve the Secure Messaging Ecosystem

"Secure messaging should be more adopted by Allied Health who rarely use it. Also searching for addressing in Medical Director extremely difficult through MD exchange. No directory of providers using other software than HealthLink and their EDIs readily available."

- Digital Health and QI Team Leader, PHN

"We need the allied health and specialists to understand that basic email is not secure enough"

- Practice Manager, General Practice

"Stage goals to prevent AHPs becoming overwhelmed:

1. Get all AHPs registered for free to RECEIVE secure messages using the provider that is most prominent in their area (e.g. in Qld - Medical Objects).
2. Get the secure messaging providers to send email alerts to the AHPs whenever there is a new secure message waiting for them to read
3. Once AHPs have some familiarity with the secure messaging system, encourage them to be able to also SEND messages by offering discounted registration
4. Work with AHPs across all disciplines to develop unified messaging templates that are easy to navigate and useful across all disciplines"

- Occupational Therapist / Lymphoedema Therapist, Allied Service

"Adoption by all"

- GP

"The largest issue is that most doctors who refer to us send referrals via fax still, rather than by Secure Messaging. It would be much more efficient if they could use Secure Messaging only. The main issue cited is that they want to send more complex docs that don't fit the restrictions for WORD formatting required - I don't think they realise that PDF documents can now be sent via SM."

- Dietitian, Allied Health Service

"We do not use it because GP practices say they cannot open it. Make it easy to open a Secure Message"

- Service Specialist Social Worker, Allied Health Service



During the analysis of the Current State, a number of challenges and themes were identified as key contributors to the current maturity of Secure Messaging Adoption

The consultation process resulted in the identification of key themes that were used to build a current state snapshot of the Secure Messaging Ecosystem. Five categories of themes were identified, with the Secure Messaging end-to-end process underpinning the whole ecosystem:



Governance

There is a **lack of governance** for the Secure Messaging process in terms of legislative, regulatory, standards frameworks and incentive schemes.



Industry

Key themes revolve around the current interactions within the vendor market and a **misaligned value proposition** for Secure Messaging across the industry.



Technical Capability

The technical capability has been proven to work but there are **variations** in sender and receiver **formats**, a **lack of trust** in exchanging PKI certificates and **data challenges** around provider directories.



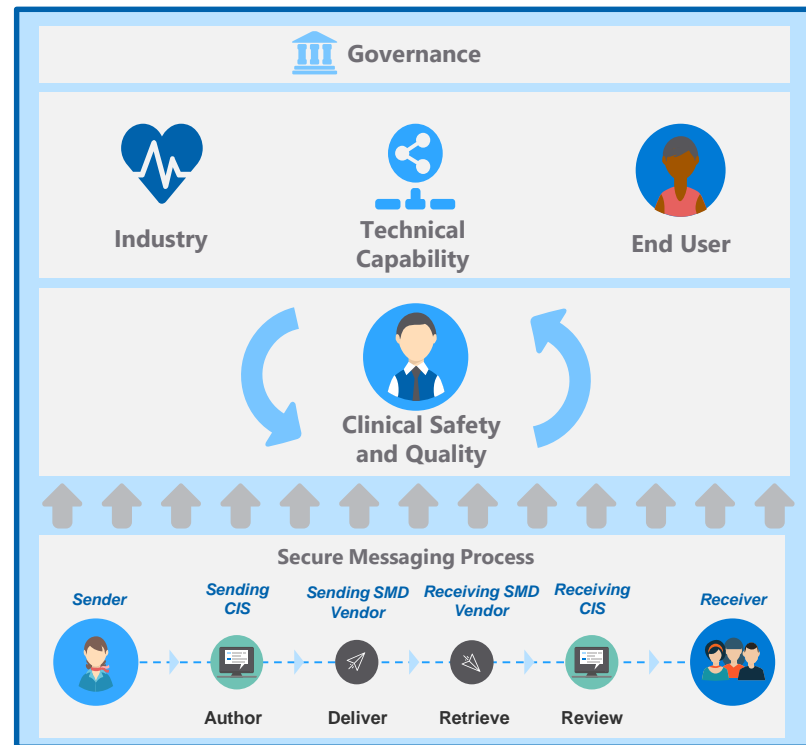
End User

End users find the **user experience** of sending a Secure Message to be **complex and time consuming**.

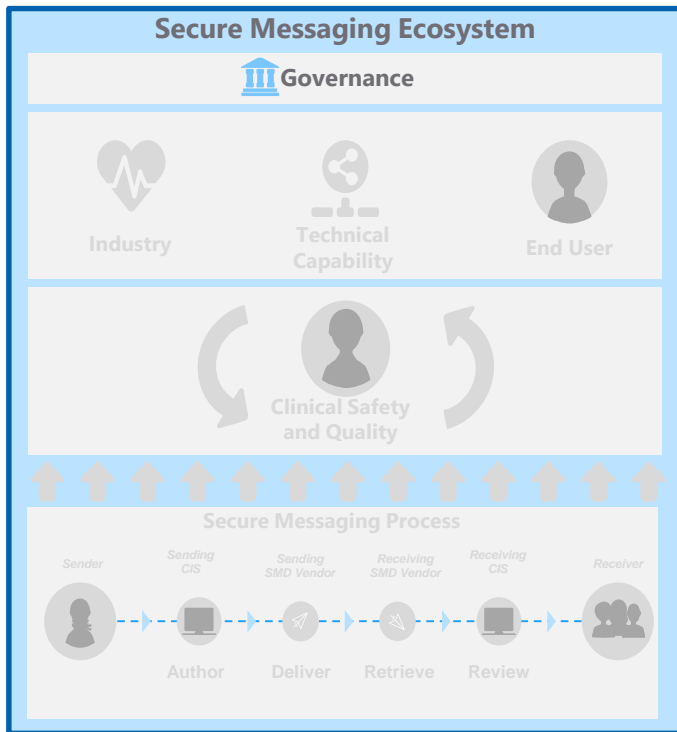


Clinical Safety and Quality

Patient **data is compromised and the continuum of care** is negatively impacted due to end users following **manual workflows** (i.e. using fax or printing to communicate), instead of using Secure Messaging.



Minimal oversight by governing bodies contribute to a lack of commonality and standardisation across the end-to-end Secure Messaging process



Governance

There is currently an opportunity to strengthen the governance around the use of Secure Messaging across various levels of the Secure Messaging Ecosystem. Further challenges are summarised as below:

- There is an opportunity to establish a federal governing body providing detailed requirements for the compliance to Secure Messaging standards. i.e. CIS and SMD vendors are using different standards to send and receive messages between each other, resulting in messages not reaching their intended destination
- There is no message payload or template framework that provides a clear understanding of acceptable message payloads and templates between vendors. Currently, different CIS vendors assemble payloads inconsistently and this impacts on the sending and receiving of content i.e. what a sender generates may not be able to be processed and presented in a receiving CIS. In extreme cases, this may mean that messages are rejected by SMD vendors. It should be noted that SMD itself is content agnostic. However, standardising content is important to support end-to-end interoperability

Note that the messaging payload using HL7v2.4 and CDA are part of the current industry offer that was released on March 2019¹, with testing tools to confirm correct implementation of these specifications

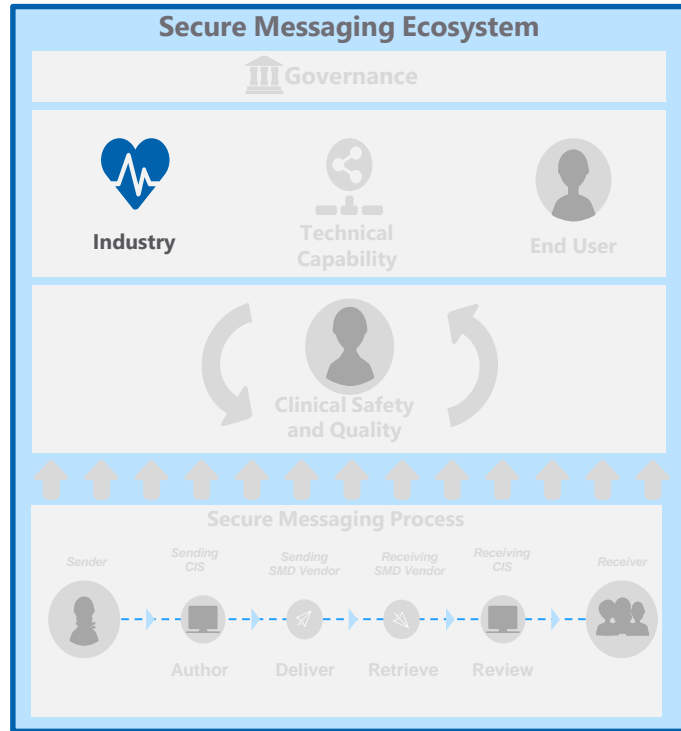
- There are no clear incentive frameworks or schemes in place for end users, SMD and CIS vendors. Current incentive schemes (e.g. ePIP) for end users do not directly support sector wide Secure Messaging adoption

Sources

1. Secure Messaging incentive for clinical software vendors (<https://www.digitalhealth.gov.au/about-the-agency/tenders-and-offers/secure-messaging-incentive-for-clinical-software-vendors>)



There is an opportunity for CIS and SMD vendors to be interoperable. This can be observed across some vendors. However, is not consistent across the entire sector



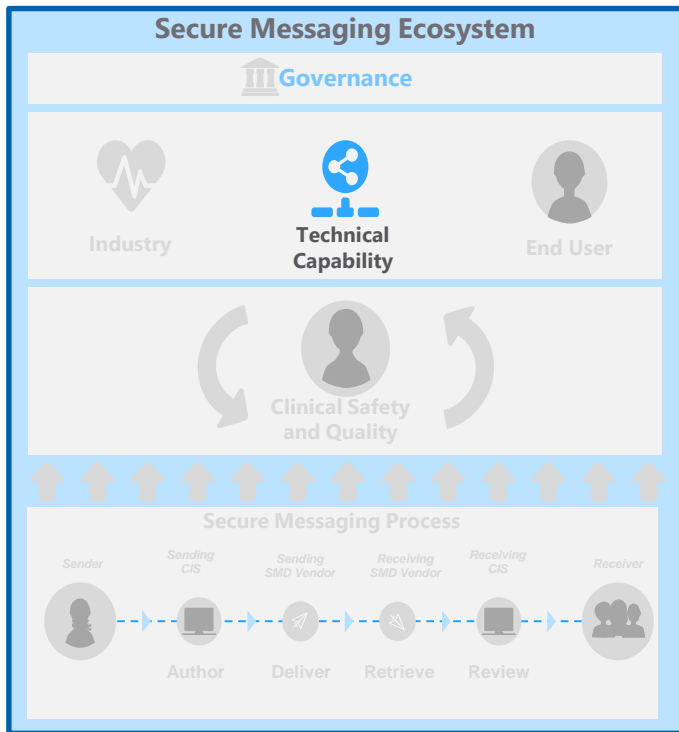
Industry

The overall value proposition of Secure Messaging is not consistent across the healthcare industry which includes the CIS and SMD vendors, Peak bodies (e.g. MSIA, RACGP, AMA, RACS and others) and other government bodies such as CSIRO. Further challenges are summarised as below:

- Peak body support for Secure Messaging is varied due to a misaligned understanding of the value proposition
- The requirements for the current ADHA industry offer is perceived as being unclear, with some vendors choosing not to participate, prioritise or invest in developing their software. Coupled, with a lack of adequate financial incentives for the vendors to cover the cost of development, mean overall vendor involvement is varied
- A number of vendors perceive that projects such as the current market offering (involved in uplifting Secure Messaging capabilities), are not aligned with what their customers require. It is challenging for them to prioritise this on their development roadmap
- CIS vendors believe that point-to-point connection between other CIS vendors will help alleviate existing pain points with the Secure Messaging process
- While some SMD vendors have achieved interoperability through bipartisan agreements, not all vendors have achieved this. There is a limited number of commercial agreements to support interoperability as interoperability is seen as a threat to existing market share held by the vendors, and these are of potential concern to the ACCC when this approach is taken rather than standards compliance
- The CIS vendor landscape and industry are developing future solutions including cloud service offerings that use FHIR standards. It is perceived that this will help overcome some of the current challenges with the current Secure Messaging process
- There are no agreed deadlines, frameworks or a set of requirements for vendors to work within, to deliver Secure Messaging successfully
- A new national solution is not favoured by vendors as it is perceived that there is currently a lack of infrastructure to support this solution



Secure Messaging has been proven to technically work. However, technical issues identified with interoperability and message payloads remain an issue due to the absence of agreed standards



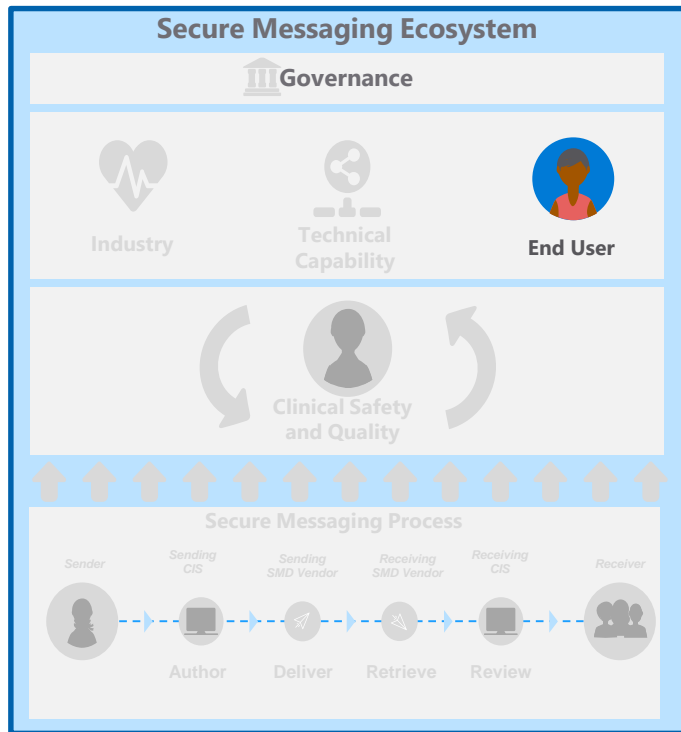
Technical Capability

Secure Messaging technology has been proven to work however, vendors still face technical challenges. Further challenges are summarised below:

- There is limited interoperability across SMD vendors, which means healthcare organisations need to install more than one messaging agent to communicate
- There are instances where messages are not received at all or cannot be opened due to the variations between acceptable sender and receiver formats. e.g. a receiving GP systems may crash due to a message that contains a large image or file in the message payload. There are further challenges in transforming messages securely from one CIS / SMD system to another. Variety of CIS and SMD vendors are using variations of HL7 standards
- Message acknowledgement capability is immature or not easily visible
- There are challenges with attaching PDF documents or images as required by specific Use Cases
- There is a lack of monitoring or incident management supporting the Secure Messaging process
- Address books are not consolidated, which results in the user having to search multiple address books to locate the address of the message recipient. Address books are also not maintained and up-to-date information is unavailable
- The process of getting a NASH certificate is perceived by some, as taking too long, challenging to set up and the renewal of certificates create an administration overhead
- There is a lack of trust in the transfer and acceptance of PKI certificates between some vendors
- Implementation of processes that can test the Secure Messaging solutions developed by CIS and SMD vendors, need to be developed or finalised



End users perceive Secure Messaging to be fundamentally broken and continue to revert to manual processes, such as faxing to transfer clinical data, because it is easier and faster



End User

End users are users who use CIS and SMD vendors to send clinical information via Secure Messaging. This includes (but is not limited to) General Practitioners, Pathology, Imaging, Hospitals, Specialists etc. Patient care is the priority for end users, however end users are inherently time poor and tend to take the 'path of least resistance' with regards to administrative tasks that they need to perform. Further challenges are summarised below:

- The solution is complex to set up, as there are multiple SMD vendors that need to be connected to a single CIS
- There are multiple steps that need to be undertaken in order to send a Secure Message within the CIS, and the user experience is not streamlined. End users end up reverting back to using printers (e.g. for providing a referral to the patient), emails or fax because it is currently quicker to do so and often easier
- End users have to search multiple address books to locate the most up-to-date address of the recipient
- Once the message is sent, there is a lack of visibility of whether the message has been received and triaged by the intended recipient. Also some end users may be able to receive Secure Messages from other end points but may not be able to send a Secure Message to the intended recipient
- End users are not motivated to use Secure Messaging as there is a lack of perceived benefit. An ePIP incentive was offered to GPs' in 2013 to install a Secure Messaging system, however the incentive was not based on demonstrating outcomes such as the regular exchange of Secure Messages in a standards based format
- End users who have not received an incentive often have a lower level of technical capability and may not have a CIS or PMS, are not inclined to use Secure Messaging. This impacts the value proposition of Secure Messaging to an individual provider as the network of 'people to talk to' is small
- Current Secure Messaging solutions do not consider all Use Cases across the healthcare sector (e.g. Allied Health practitioners). It also does not cater for all types of healthcare services including those that do not have a provider number, yet provide services
- Secure Messaging adoption rates is varied by region, healthcare provider type, whether an end user was a sender or receiver and the amount of patients they serviced



Patients expect their data to be digitally exchanged between healthcare providers, in a timely and secure manner, to enable the continuum of care



Clinical Safety and Quality

Patient clinical safety and quality is negatively impacted by the lack of timeliness of patient clinical information not being securely exchanged between healthcare providers. Patients expect that their data is shared securely between healthcare providers, in order to support the continuum of care. Further challenges are summarised below:

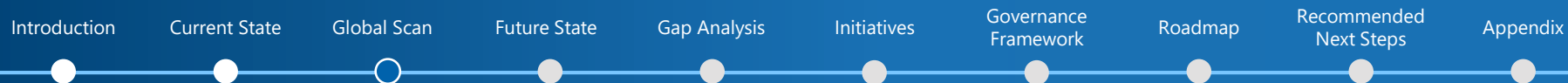
- The traditional clinical workflow has not deviated. In some instances, end users are still currently providing their patients with a paper based copy of a referral or specialist letter which may be misplaced by the patient
- There is a risk that patient data and confidentiality is compromised as a result of clinical information being sent to incorrect end points, either via email, fax or print outs
- Patients currently spend time "retelling the story" due to the lack of up-to-date clinical information being successfully sent to the current consulting healthcare provider¹
- When an end user utilises CDA level 1 or 2 messages to capture patient information in their CIS, the messages may be sent as attachments rather than being correctly coded. This will require manual transcription into the CIS which raises potential for human error. This means that the patients' information is captured incorrectly and accuracy is compromised
- Due to the lack of standardised Secure Messaging acknowledgements, many end users revert to manual processes such as a phone call or fax in order to confirm the transfer of care

Sources

1. Strategic Priorities (<https://conversation.digitalhealth.gov.au/secure-messaging>)



Global Scan



Globally, there are various initiatives, programs and organisations that are focused on reducing manual and paper-based workflows across their respective healthcare sectors



CANADA

Canada Health Infoway continues to provide national leadership in interoperability standards in 2018-2019. The HL7 Canada community, with participation and support from Infoway, is leading a pan-Canadian FHIR baseline profile to support a common approach to the use of FHIR profiles in Canada



UNITED STATES

- The **Meaningful Use** program rolled out in 2011 and require physicians using certified electronic health records technology (CEHRT) to capture, exchange and report specific clinical data and quality measures
- **DirectTrust** is a collaborative non-profit association (containing health IT and healthcare provider organisations) to support secure, interoperable health information exchange via the direct message protocols. They have also established the DirectTrust framework for the exchange of Secure Messages



AUSTRALIA

- There are significant pockets of Secure Messaging in use with varying degrees of success. Western Victoria Primary Health Network reports that in the **Barwon** region, clinicians are sending Secure Messages via systems like ReferralNet and Argus
- Industry collaboration sessions and proof of concepts that included vendors, prove that Secure Messaging can work at a technical level



UNITED KINGDOM

The National Health Service Trust has launched a national campaign to **"Axe the Fax"** with an aim to decommission 95% of fax machines used by various healthcare providers. This was in response to the government providing NHS a deadline of March 2020, which mandated the elimination of the use of fax machines from the UK healthcare system



In Canada, healthcare delivery is managed and funded by each province, with independent organisations providing guidance on accreditation and standardisation

Secure Messaging is consolidated into EMR or patient portal technologies. The below, are examples of how some organisation's in Canada are managing aspects of the Secure Messaging process



Accreditation Canada¹

- Accreditation Canada is a not-for-profit organisation that is dedicated to working with patients, policy makers and the public to improve the quality of health and social services for all
- They are affiliated with the Health Standards Organisation (HSO) to deliver more objective, credible and outcome-oriented assessment programs based on the best global standards
- An applicable standard such as HSO 83001:2018 (E), Virtual Health Standard applies to all health service organisations that receive and/or deliver Virtual Health (which covers clinical information exchange between patients and providers), and is one of the many standards that Accreditation Canada uses to assess healthcare providers

Infoway²

- Canada Health Infoway (Infoway) helps to improve the health of Canadians by working with partners to accelerate the development, adoption and effective use of digital health across Canada
- Infoway continues to provide national leadership in interoperability standards in 2018-2019. The HL7 Canada community, with participation and support from Infoway, is leading a pan-Canadian FHIR baseline profile to support a common approach to the use of FHIR profiles in Canada
- As the National Release Centre (NRC) for a number of messaging and vocabulary standards, Infoway continued its' important role of ensuring that health information is standardised and shareable. In addition to providing standards licensing, access, maintenance and implementation support to every jurisdiction, the NRC published approximately 30 releases with more than 1,000 content changes in support of digital health solution implementations in Canada, including immunisation

Lessons learnt

- Accreditation processes can provide a framework for Secure Messaging solutions to meet standardisation requirements. End users are more likely to trust accredited solutions
- Presence of national leadership and a common approach to establishing standards is critical for driving interoperability between vendors

Sources

1. Accreditation Canada (<https://accreditation.ca/intl-en/accreditation/qmentum/>)

2. Canada Health Infoway (<https://infoway-inforoute.ca/en/>)

Note: Information was sourced from desktop research



In the United States, organisations such as DirectTrust are promoting standardisation through trust frameworks and national programs such as Meaningful Use to monitor compliance

The healthcare sector in the United States is predominately private providers with a large multitude of vendors servicing the market. The Meaningful Use program drove the establishment of a DirectTrust association and framework, which helped support provider-to-provider and provider-to-patient exchange of messages.

Meaningful Use - Centers for Medicare & Medicaid Services (CMS)¹

- CMS developed an incentive program called Meaningful Use (MU) in 2011, requiring physicians using certified electronic health records technology (CEHRT) to capture, exchange and report specific clinical data and quality measures. This program was divided into the following stages:
 - Stage 1 established the base requirements for electronic capturing of clinical data
 - Stage 2 encouraged the use of electronic health records for increased exchange of information and continuous quality improvement at the point of care. Modified Stage 2 (released in October 2015) consolidated Stages 1 and 2 into a new program. These are the current requirements all physicians should follow. While some changes were made to reduce the complexity of the measures, many of the objectives were carried over from Stage 2
- Physicians who fail to participate in MU will receive a penalty in the form of reduced Medicare reimbursements. Physicians must use certified electronic health records technology (CEHRT) and demonstrate MU through an attestation process at the end of each MU reporting period to avoid the penalty

DirectTrust²

- DirectTrust is a collaborative non-profit association (containing health IT and healthcare provider organisations) to support secure, interoperable health information exchange via the direct message protocols
- This trust framework supports both provider-to-provider direct exchange and bi-directional exchange between consumers/patients and their providers
- The common goal of DirectTrust members is to establish and maintain a national, transparent Security and Trust Framework upon which trust relationships for exchange technology can be scaled and federated nationally

Lessons learnt

- Providing incentives for using Secure Messaging solutions or introducing penalties for non-compliance may increase Secure Messaging adoption
- A trust framework between organisations can facilitate the exchange of clinical information between healthcare providers in an efficient and secure manner

Sources

1. Meaningful Use: Electronic Health Record (EHR) incentive programs (https://www.ama-assn.org/practice-management/medicare/meaningful-use-electronic-health-record-ehr-incentive-programs#related_links-1)

2. What is DirectTrust (<https://www.directtrust.org/about-directtrust/>) –

Note: Information was sourced from desktop research



In the UK, the “Axe the Fax” campaign has been mandated in order to remove fax communications and support streamlined, paper-less clinical workflows

The UK has committed to completely eradicate the use of fax machines throughout the healthcare system by 2020. The National Health Service (NHS) currently operates over 9000 fax units, as many organisations within the industry require documents to be transmitted by fax.



Leeds Teaching Hospital NHS Trust¹

- The NHS Trust has previously launched a national campaign to “Axe the Fax” with an aim to decommission 95% of fax machines used by various healthcare providers. This was in response to the government giving NHS a deadline of March 2020, which is driving the elimination of the use of fax machines entirely from the UK healthcare system
- The campaign initially aimed to continue to raise awareness and drive stakeholder engagement within Leeds Teaching Hospital in order to advance their own mission and also to position Leeds as a leading light in the digital health agenda. It then went on to provide other NHS Trusts with tools and support¹
- Alternative solutions to replace current faxing capabilities are being explored. One solution that has been suggested is digital / cloud faxing solutions. Fax documents can still be sent and received, and even communicated to fax machines if necessary, but the process is carried out entirely through digital, computer and smart device platforms

Lessons learnt

- A federally mandated go-live date can fast track the Secure Messaging industry to address key challenges and the demand for Secure Messaging can be driven by the end users
- Campaigns can be used effectively to raise awareness on the benefits of Secure Messaging which can phase out the use of manual workflows that are used to exchange clinical information

Sources

1. Axe the Fax Case Study (<https://www.silver-buck.com/wp-content/uploads/2018/10/ATF-Case-study-FINAL.pdf>)

Note: Information was sourced from desktop research



In Australia, the drivers behind the pockets of Secure Messaging success can be analysed for opportunities that can be applied across the country

The pockets of success in Australia are due to a varied range of electronic communication methods, for example, diagnostic requesting and reporting, and the sending of discharge summaries from hospitals to general practice. However, these different methods are generally not compatible as these approaches work independently of each other.

Pockets of success in the Barwon Region

- Western Victoria Primary Health Network reports that in the Barwon region, clinicians sending Secure Messages via systems like ReferralNet and Argus are securely sending an average of 16 000 messages per month, thus saving time, money and effort. The number of messages sent each month continues to grow as clinicians incorporate this function into their daily work routine¹

Industry collaboration between Telstra Health and Global Health

- Telstra Health (a CIS and SMD vendor) and Global Health (a CIS and SMD vendor) have achieved two-way interoperability to securely transfer patient information between healthcare providers²
- Following a 12 month collaboration between the two parties (which also included engagement with a broad range of clinical software vendors) healthcare providers can now securely and electronically exchange clinical information. This includes referrals, progress notes, specialist letters, discharge summaries, diagnostic results and home medicine reviews



Lessons learnt

- Pockets of success in Australia demonstrate that the technical capability of Secure Messaging is achievable
- A collaborative approach between ADHA, vendors, industry leaders and governing bodies can promote goodwill and a willingness for vendors to work together towards interoperability

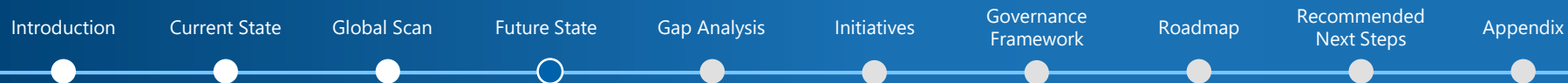
Sources

1. National Digital Health Strategy
2. Telstra Health
(<https://www.telstrahealth.com/home/news-and-insights/telstra-health-and-globalhealthworktogethertoachievepatientsecure.html>)

Note: Information was sourced from desktop research



Future State



The Secure Messaging vision statement is stipulated in Australia's National Digital Health Strategy and will be used as a reference for success



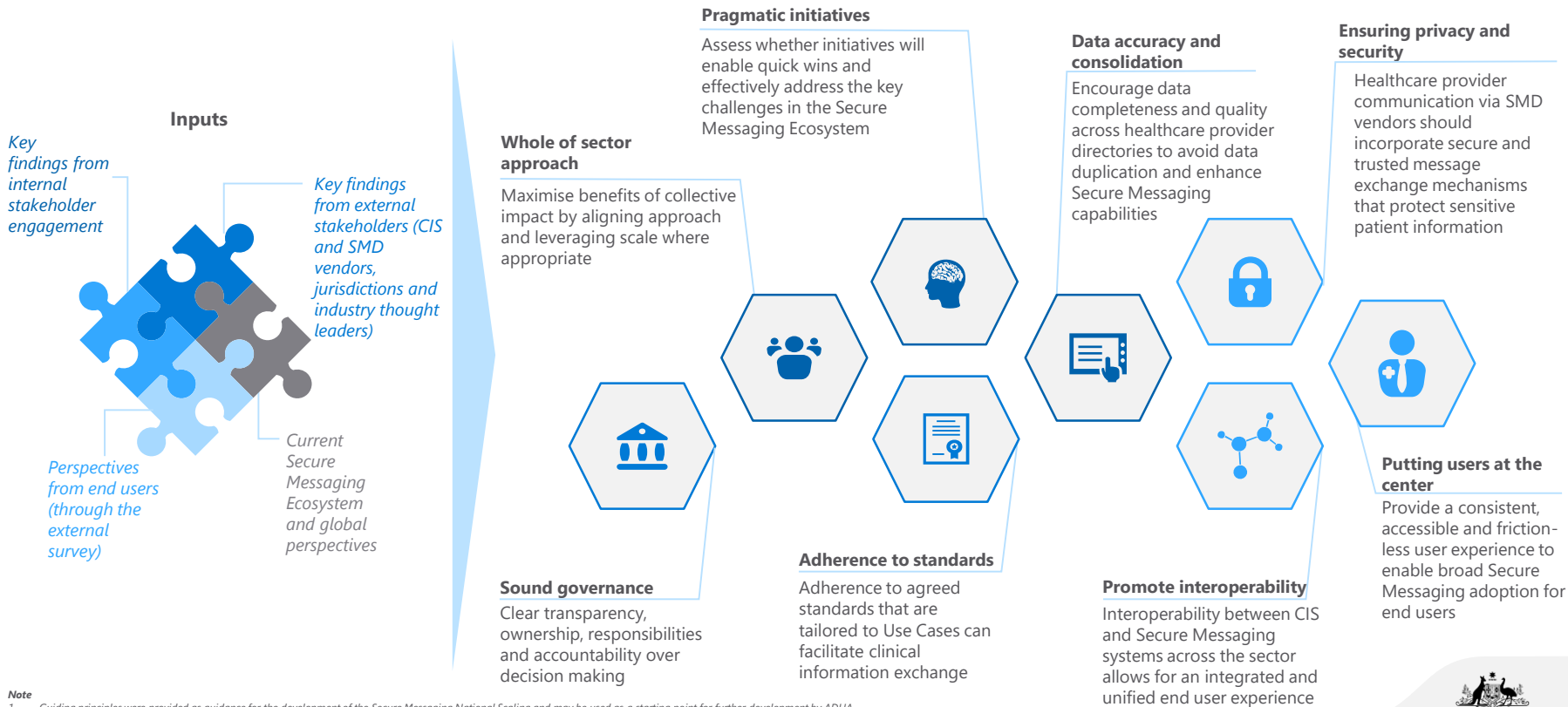
“Every healthcare provider will have the ability to communicate with other professionals and their patients via secure digital channels if they so choose. This will end dependence on paper-based correspondence and the fax machine or post.”

- Australia's National Digital Health Strategy

NB: This engagement focuses on secure digital communications between healthcare providers



Based on inputs from ADHA internal and external (vendors and industry) perspectives, eight guiding principles were identified to support the development of the future state



The future state Secure Messaging Ecosystem will have defined governance, interoperability between vendors, technical capability uplift and enable end users to focus on the patient

What does the future state of the Secure Messaging Ecosystem look like?



Governance

Governance has been established across the Secure Messaging Ecosystem. Roles and responsibilities have been defined, standardisation requirements and conformance across the end-to-end Secure Messaging process have been mandated. Funding requirements have been agreed and accreditation processes have been developed and mandated.



Industry

By using the mandated standards as guidelines, CIS and SMD vendors are able to collaborate and co-design with each other. As a result SMD vendors are interoperable with each other and subsequently Secure Messaging adoption has increased. Hence, the value proposition for Secure Messaging is being realised across the healthcare sector.



Technical Capability

Message payload and templates are aligned to Use Case requirements, the process for NASH certificates is streamlined and PKI Trust frameworks have been implemented. Message acknowledgement, incident management and monitoring capabilities have been implemented. An up-to-date federated directory has been implemented. Additionally testing processes have been established to assess against the Standards Framework.



End User

Use Cases for end users are well defined and informs the technical requirements for the Standards Framework and message templates. End user experience is streamlined and clear lever schemes have increased the adoption of Secure Messaging.

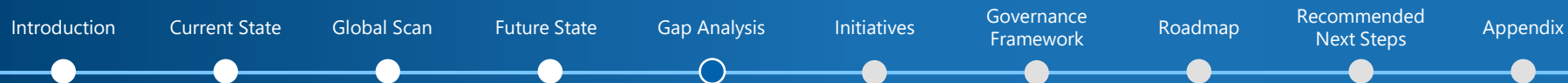


Clinical Safety and Quality

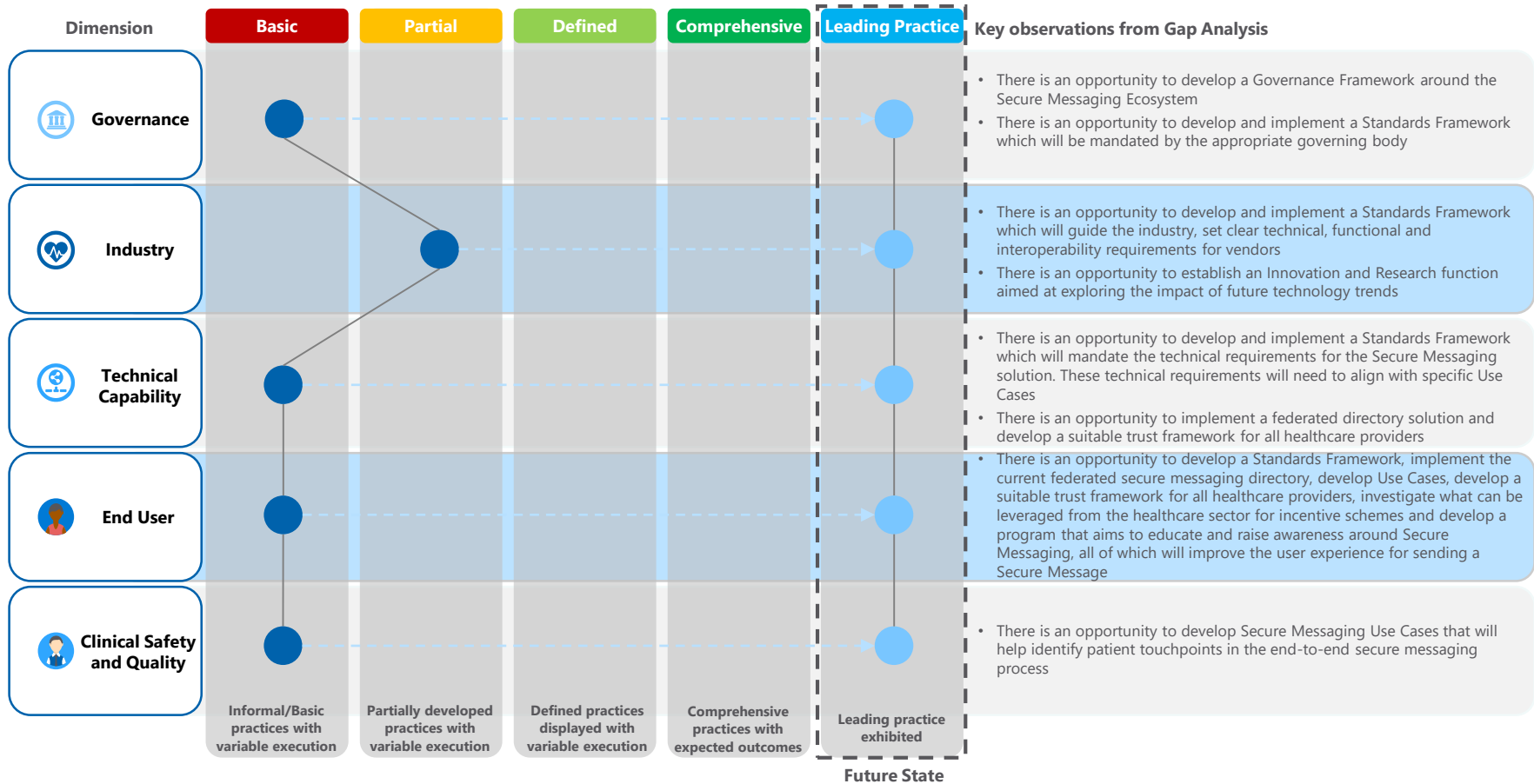
Patient focussed clinical safety and quality is enhanced due to the benefits of Secure Messaging. Patients do not spend time “retelling the story” and feel assured by the security and confidentiality of clinical information exchange via Secure Messaging.



Gap Analysis



A comparison between the current and the future state, presented various opportunities to improve at each dimension of the Secure Messaging Ecosystem



Detailed gap analysis | The Governance dimension



Current State	Future State	Gap Analysis
There is an opportunity to establish a federal governing body providing detailed requirements for the compliance to Secure Messaging standards. i.e. CIS and SMD vendors are using different standards to send and receive messages between each other, resulting in messages not reaching their intended destination.	There is established governance around the Secure Messaging Ecosystem. Roles and responsibilities have been agreed and adhered to. Oversight is maintained and all contributing factors of the Secure Messaging Program is managed.	There is an opportunity to develop governance around the Secure Messaging Ecosystem. Roles and responsibilities need to be developed and communicated to the appropriate governing bodies.
There is no message payload or template framework that provides a clear understanding of acceptable message payloads and templates between vendors. Currently, different CIS vendors assemble payloads inconsistently and this impacts on the sending and receiving of content i.e. what a sender generates may not be able to be processed and presented in a receiving CIS. In extreme cases, this may mean that messages are rejected by SMD vendors. It should be noted that SMD itself is content agnostic. However, standardising content is important to support end-to-end interoperability.	Acceptable message payloads or template frameworks have been agreed and adhered to. Vendors are able to configure their CIS or SMD using the message payload or template frameworks, hence allowing interoperability with each other.	There is an opportunity to develop standardisation and conformance around the message payloads by agreeing on message payload or template frameworks. <i>Note that the messaging payload using HL7v2.4 and CDA are part of the current industry offer that was released on March 2019, with testing tools to confirm correct implementation of these specifications¹</i>
There are no clear incentive frameworks or schemes in place for end users, SMD and CIS vendors. Current incentive schemes (e.g. ePiP) for end users do not directly support sector wide Secure Messaging adoption.	Funding requirements have been finalised and relevant lever frameworks have been agreed upon. End users are incentivised to send a Secure Message hence increasing adoption.	There is an opportunity to develop a lever framework which may reward end users for sending a Secure Message and for CIS and SMD vendors for meeting standardisation requirements (e.g. through accreditation). Further exploration is required for the current lever frameworks being used across the healthcare industry, so it can be leveraged to reward the appropriate stakeholder.

Sources

1. Secure Messaging incentive for clinical software vendors (<https://www.digitalhealth.gov.au/about-the-agency/tenders-and-offers/secure-messaging-incentive-for-clinical-software-vendors>)



Detailed gap analysis | The Industry dimension



Current State	Future State	Gap Analysis
Value proposition of Secure Messaging is not consistent across the healthcare sector.	Value proposition for Secure Messaging is realised (after the end-to-end challenges have been addressed) and there is an increase in adoption.	There is an opportunity to raise awareness and promote the use of Secure Messaging through a change and adoption program.
The requirements for the current ADHA industry offer is perceived as being unclear, with some vendors choosing not to participate, prioritise or invest in developing their software. Coupled, with a lack of adequate financial incentives for the vendors to cover the cost of development, mean overall vendor involvement is varied.	Industry offers have clear requirements and criteria to be met that align with industry standards, hence guiding solution development for vendors. Incentives (such as accreditation) are offered to vendors who meet the industry offer requirements and vendors are able to prioritise relevant development projects on their roadmaps.	There is an opportunity to develop a standards framework which will define the requirements for Secure Messaging solution development and inform future industry offer requirements.
A number of vendors perceive that projects such as the current market offering (involved in uplifting Secure Messaging capabilities), are not aligned with what their customers require. It is challenging for them to prioritise this on their development roadmap.	As a standards framework has been established, and industry offers have clearly defined requirements, vendors are able to incorporate additional Secure Messaging projects or programs into their development roadmaps and prioritise them accordingly.	There is an opportunity to develop a standards framework that will define the requirements for Secure Messaging. Industry offering requirements will reflect additional development of the Standards Framework and assist vendors in incorporating these projects into their respective roadmaps.
CIS vendors believe that point-to-point connection between other CIS vendors will help alleviate existing pain points with the Secure Messaging process.	CIS vendors can collaborate and co-design with SMD vendors to develop enhancements and customisations to the Secure Messaging capability. Standards frameworks are used to guide development.	There is an opportunity to develop a standards framework which will define the requirements for the Secure Messaging solution development, and can be used by vendors to guide their development activities.
While some SMD vendors have achieved interoperability, not all vendors have achieved this. There is a limited number of commercial agreements to support interoperability as interoperability is seen as a threat to existing market share held by the vendors.	SMD vendors have all achieved interoperability and have commercial agreements with each other to support interoperability.	There is an opportunity to develop a governance framework that enables interoperability between vendors, and develop a standards framework that when adhered to, will encourage commercial agreements between a wider group of vendors.
The CIS vendor landscape and industry are developing future solutions including cloud service offerings that use FHIR standards. It is perceived that this will help overcome some of the current challenges with the current Secure Messaging process.	Secure Messaging capability has matured and evolved to meet cloud solution requirements.	There is an opportunity to establish an innovation and research function aimed to explore the impact of future technology trends such as cloud solutions, on the current Secure Messaging capability.
There are no agreed deadlines, frameworks or a set of requirements for vendors to work within, to deliver Secure Messaging successfully.	Clear requirements for Secure Messaging capability uplift have been finalised and Go-live dates have been announced through the appropriate governing body.	There is an opportunity to develop a standards framework which will define the requirements for Secure Messaging solution development and announce deadlines for requirements to be met.
A new national solution is not favoured by vendors as it is perceived that there is currently a lack of national infrastructure to enable this solution.	Vendors are interoperable with each other due to using a mandated standards framework and there is no requirement for a national infrastructure stack to enable a Secure Messaging solution.	There is an opportunity to develop a governance framework that enables interoperability between vendors as a key requirement, and develop a standards framework that when adhered to, will encourage commercial agreements between a wider group of vendors.



Detailed gap analysis | The Technical Capability dimension



Current State	Future State	Gap Analysis
There is limited interoperability across SMD vendors, which means healthcare organisations need to install more than one messaging agent to communicate.	An end user will not require the installation of more than one messaging agent due to SMD vendors being interoperable with each other.	There is an opportunity to develop a standards framework which will mandate the requirement for SMD vendors being interoperable with each other.
There are instances where messages are not received at all or cannot be opened due to the variations between acceptable sender and receiver formats. e.g. a receiving GP systems may crash due to a message that contains a large image or file in the message payload.	Messages will be successfully received in it's intended format and without any alteration to the message format.	There is an opportunity to develop a standards framework which will mandate conformity across agreed standards for message payloads. Note that this is being addressed by the current industry offer
Message acknowledgement capability is immature or not easily visible.	The sender will be able to receive a message acknowledgement, once a message has been sent to the intended recipient.	There is an opportunity to develop a standards framework which will mandate the requirement for message acknowledgements being incorporated into Secure Messaging. Note that this is being addressed by the current industry offer
There are challenges with attaching PDF documents or images as required by specific Use Cases.	The end user is able to attach a PDF document or images as the appropriate standards have been aligned with the specific Use Case.	There is an opportunity to develop Secure Messaging Use Cases for the incorporation of PDF documents / images which will help inform the standards framework. Note that this is being addressed by the current industry offer
There is a lack of monitoring or incident management supporting the Secure Messaging process.	Incident management and monitoring processes have been implemented by the appropriate governing body. These processes are further supported by the vendors.	There is an opportunity to develop a governance framework that will detail the requirements for incident management and monitoring processes, by the appropriate party.
Address books are not consolidated, which results in the user having to search multiple address books to locate the address of the message recipient. Address books are also not maintained and up-to-date information is unavailable.	There is access to an up-to-date federated address book in which the end user is able to quickly and accurately search the recipients details.	There is an opportunity to implement a federated secure messaging directory solution where address books are up-to-date and common data identifiers support data matching and linking.
The process of getting a NASH certificate is perceived by some, as taking too long, challenging to set up and the renewal of certificates create an administration overhead.	The process to obtain, install and maintain a NASH certificate is streamlined. Non-eligible healthcare provider organisations, individual providers or supporting organisations are able to leverage a PKI trust framework which allow the acceptance of PKI certificates between senders and receivers.	There is an opportunity to review NASH processes and further develop a suitable trust framework so all PKI certificates used within the Secure Messaging Ecosystem is trusted and accepted.
There is a lack of trust in the transfer and acceptance of PKI certificates between some vendors.	The process to obtain, install and maintain a NASH certificate is streamlined. Vendors are required to use NASH as it's the "gold standard". Any exceptions will follow the PKI trust framework pathway.	There is an opportunity to develop a standards framework which will mandate the requirement to use NASH certificates or be incorporated into a suitable trust framework.
Implementation of processes that can test the Secure Messaging solutions developed by CIS and SMD vendors, need to be developed or finalised.	Testing processes and acceptance criteria have been developed around the standards framework. CIS and SMD vendors are able to test their solutions against defined criteria.	There is an opportunity to develop testing processes, associated tools and acceptance criteria hence guiding the development of future Secure Messaging solutions by CIS and SMD vendors.



Detailed gap analysis | The End User dimension



Current State	Future State	Gap Analysis
The solution is complex to set up, as there are multiple SMD vendors that need to be connected to a single CIS.	As all SMD vendors have achieved interoperability, end users only need to set up one SMD vendor at their CIS end point.	There is an opportunity to develop a governance framework which will mandate the requirement for SMD vendors to be interoperable with each other.
There are multiple steps that need to be undertaken in order to send a Secure Message within the CIS, and the user experience is not streamlined.	Due to an uptake in Secure Messaging adoption, CIS vendors have streamlined the user experience for sending a Secure Message.	There is an opportunity to develop Secure Messaging Use Cases and incorporate specific end user requirements into streamlining the user experience.
End users have to search multiple address books to locate the most up-to-date address of the recipient.	Users have one single pathway to search an intended message recipient on a federated and up-to-date directory.	There is an opportunity to implement a federated secure messaging directory solution where address books are up-to-date and common data identifiers prevent data duplication. End users also can be educated through the Change and Adoption program on the use of the federated directory solution.
Once the message is sent, there is a lack of visibility of whether the message has been received and triaged by the intended recipient. Also some end users may be able to receive Secure Messages from other end points but may not be able to send a Secure Message to the intended recipient.	The sender will be able to receive a message acknowledgement, once a message has been sent to the intended recipient.	There is an opportunity to develop a standards framework which will mandate the requirement for message acknowledgements being incorporated into Secure Messaging.
End users are not motivated to use Secure Messaging as there is a lack of perceived benefit.	End users are able to use Secure Messaging as there is an uptake of secure and efficient provider to provider communication. There are multiple levers across the healthcare industry that encourage end users to use Secure Messaging.	There is an opportunity to develop a lever framework which will drive adoption of Secure Messaging. End users can also be educated through the change and adoption program in order to promote the value proposition of Secure Messaging.
End users who have not received an incentive often have a lower level of technical capability and may not have a CIS or PMS, are not inclined to use Secure Messaging.	A clear levered incentive framework will motivate Specialists to install a CIS and begin using the Secure Messaging functionality. Specialists will be able to understand the benefits through the continuous use of secure messaging.	There is an opportunity to develop a lever framework which will reward end users for sending a Secure Message. End users can also be educated through the Change and Adoption program in order to promote the value proposition of Secure Messaging.
Current Secure Messaging solutions do not consider all Use Cases across the healthcare sector (e.g. Allied Health practitioners). It also does not cater for all types of healthcare services including those that do not have a provider number, yet provide services.	The Secure Messaging solution has evolved and meets the requirements of all major Use Cases across the healthcare sector.	There is an opportunity to develop Secure Messaging Use Cases and align the solution to major Use Cases. There is also opportunity to streamline NASH, and use commercial certificates underpinned by an suitable trust framework.
Secure Messaging adoption rates is varied by region, healthcare provider type, whether an end user was a sender or receiver and the amount of patients they serviced.	Secure Messaging adoption rates are high and consistent across regions, healthcare provider types, whether an end user was a sender or receiver and regardless of the amount of patients they serviced	There is an opportunity to develop Secure Messaging Use Cases that aim to understand and document the rates of adoption for end users, as well as understand the volumes of message exchanges.



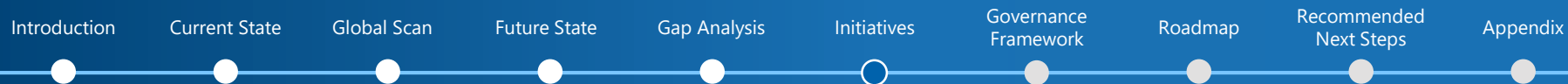
Detailed gap analysis | The Clinical Safety and Quality dimension



Current State	Future State	Gap Analysis
The traditional clinical workflow has not deviated. In some instances, end users are still currently providing their patients with a paper based copy of a referral or specialist letter which may be misplaced by the patient.	The patient is able to also receive a digital notification of a relevant Secure Message (e.g. copy of an eReferral) through a digital device (e.g. mobile). The end user is able to successfully send an eReferral to the intended recipient.	There is an opportunity to develop a lever framework which will reward end users for sending a Secure Message. End users can also be educated through the change and adoption program in order to promote the value proposition of Secure Messaging. An innovation and research focused function can assess the feasibility of developing interoperability between CIS and mobile device platforms.
There is a risk that patient data and confidentiality is compromised as a result of clinical information being sent to incorrect end points, either via email, fax or print outs.	Patient data and confidentiality is protected due to security and data protection controls around the sending and receiving of a Secure Message.	There is an opportunity to implement a standards framework which will mandate the requirement to use NASH certificates or be incorporated into a suitable trust framework (where providers and vendors who don't qualify for NASH are able to use commercial certificates or an appropriate alternative). There is also an opportunity to implement a reliable federated address book where senders can locate an accurate receiver end point. The implementation of the opportunities above can enable the security and confidentiality of patient data. Note that NASH and commercial certificates are currently being used.
Patients currently spend time "retelling the story" due to the lack of up-to-date clinical information being successfully sent to the current consulting healthcare provider.	Digital communications allows the clinician the opportunity to validate the patient information and data, as opposed to starting from scratch	There is an opportunity to develop a standards framework, and implement a reliable federated address book which will improve the overall user experience in sending a Secure Message. This will have subsequent effects to support an end user adhere to clinical safety and quality.
When an end user utilises CDA level 1 or 2 messages to capture patient information in their CIS, the messages may be sent as attachments rather than being correctly coded. This will require manual transcription into the CIS which raises potential for human error. This means that the patients' information is captured incorrectly and accuracy is compromised.	Patients do not have to worry about their clinical information being transferred incorrectly or inaccurately as end users are able to send a Secure Message in a standardised format which align with their specific Use Case requirements. There is no need for further manual transcription into a required format.	There is an opportunity to develop secure messaging Use Cases which will inform the standards framework. This will enable the end user to input clinical information into standardised format which is accepted by the recipient and successfully transported by the SMD vendors.
Due to the lack of standardised Secure Messaging acknowledgements, many end users revert to manual processes such as a phone call or fax in order to confirm the transfer of care.	Patients experience a continuum of clinical care due to end users being able to successfully send a Secure Message to the recipient and have their message acknowledged.	There is an opportunity to develop a standards framework which will mandate the requirement for message acknowledgements being incorporated into Secure Messaging.



Initiatives



Through stakeholder consultation and analysis, eight key initiatives have been identified to accelerate the adoption of Secure Messaging



Develop Secure Messaging Governance Framework



Develop Secure Messaging Use Cases



Agree on Secure Messaging Standards and Develop a Standards Framework *(in progress)*



Implement a Federated Secure Messaging Directory Solution *(in progress)*



Review NASH Process and Develop a Suitable Trust Framework *(in progress)*



Establish a Change and Adoption Program



Develop a Secure Messaging Lever Framework



Establish an Innovation and Research Function

Note that this initiative is not included in the roadmap as it supports the wider National Digital Health Strategy and it is only included here as an optional initiative. However, there is applicability to the Secure Messaging program



Each recommended initiative details the estimated duration, themes addressed, key activities, initiative status, prioritisation rating, stakeholder impact and high level risks

Estimated Duration

The estimated duration indicates the amount of time required to complete the key activities of the initiative.

Themes Addressed

Themes addressed refer to the themes from the Current State Analysis that the initiative focusses on.

Key Activities

Key activities outline the events, outcomes and stakeholder interactions required for the implementation of the initiative. These activities are non-exhaustive and should be used for guidance.

Status

Status refers to the progress status of the initiative. Some recommended initiatives are currently underway, while others have not commenced.

Prioritisation Rating

The prioritisation rating provides a ranking on each initiative. The criteria for the rating is as follows:

Adoption Benefit:

Impact on Secure Messaging Adoption rates

Complexity:

- Technical impact and / or;
- End user impact and / or;
- Business impact

Prioritisation ratings were discussed and agreed during the Prioritisation workshop with key ADHA executives.

Stakeholder Impact

Stakeholder impact refers to the level of change / influence a particular initiative brings to a stakeholder group. Impact is categorised as follows:

- *Positive:* Initiative brings out a change that benefits the stakeholder group, with limited investment required from the stakeholder group.
- *Neutral:* Initiative benefits the stakeholder group but is balanced by required significant investment.
- *Negative:* Initiative has limited and direct benefit to the stakeholder group and requires investment.

Risks Assessment

The risk assessment identifies key risks associated with an initiative and is categorised as either a *development risk* or an *implementation risk*. The overall risk rating is determined by the level of impact a risk has on the Secure Messaging Program if manifested, and how likely the risk is to occur. The following risk assessment matrix was used to conclude the overall risk rating:

		Overall Risk Rating		
Risk Impact	High	Medium Risk	High Risk	High Risk
	Medium	Low Risk	Medium Risk	High Risk
	Low	Low Risk	Low Risk	Medium Risk
		Unlikely	Possible	Likely
		Probability		

Note that this risk assessment is non-exhaustive.





Develop a Secure Messaging Governance Framework

Overview | Develop a Secure Messaging Governance Framework

The Secure Messaging Governance Framework aims to provide direction and control through a set of roles and responsibilities, activities and stakeholder interactions. The framework will be used to support and maintain the oversight and management of all contributing factors of the Secure Messaging Program.

Estimated Duration

6 months

Themes Addressed



Key Activities

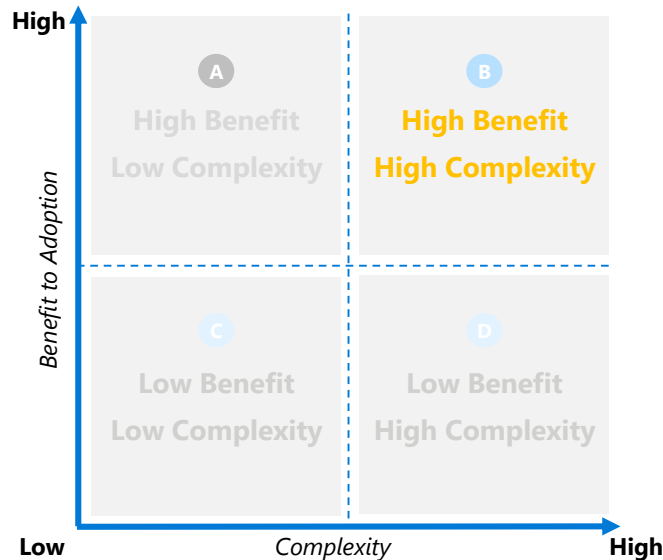
Key activities related to the Governance Framework are (but not limited to):

- Define goals and principles of the Secure Messaging Governance Framework (*completed as a part of this engagement*).
- Design Governance Structure and related activities (*completed as a part of this engagement*).
- Develop an implementation plan that includes:
 - Analysis of current state Governance processes
 - Identification of gaps between current state Governance processes and the target state Governance Framework
 - Design of “new” processes, organisational structures and roles that addresses identified gaps
 - Design of decision making and review schedules
 - Identification of reporting tools and / or design of reporting templates
 - Definition of performance metrics by which outcomes will be measured

Status

Not Started

Prioritisation Rating



This initiative was categorised as high benefit, as it influences Secure Messaging adoption rates through guidance, control and conformance. It is categorised as high complexity as it requires process changes and the allocation of roles and responsibilities.



Stakeholder Impact | Develop a Secure Messaging Governance Framework

This initiative impacts four key stakeholder groups, namely Governing Bodies, ADHA, CIS and SMD vendors and end users.

Stakeholder Impact

Stakeholder	Impact	Explanation
Governing Bodies (Dep. of Health, COAG Health Council and AHMAC)	Neutral	Decision making and mandating activities mean that governing bodies will take on the overall accountability for the success of the Secure Messaging Program.
ADHA	Neutral	ADHA will be taking on additional responsibilities in both the regulation and management activities, and will require the resources and processes to do so.
CIS and SMD vendors	Positive	Vendors will be provided the direction they require from Governing Bodies. However, they will need to incorporate additional reporting requirements into their BAU processes.
End users	Positive	End users will benefit from technical and commercial interoperability of CIS and SMD vendors, as well as the additional support and collaboration with Change Champions.



Risk Assessment | Develop a Secure Messaging Governance Framework

Overall Initiative
Risk Rating:

High

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Development and Implementation	Governing and regulating bodies reject the roles and responsibilities as there is no legislative backing by Federal Government.	High <i>Rationale:</i> Rejection of roles and responsibilities will require a redesign of the Governance Framework and may delay the design and implementation of other key initiatives.	Possible <i>Rationale:</i> Governing and regulating bodies may not be invested in the value proposition of Secure Messaging.	High	Facilitate conversations to understand the reasons for rejecting roles and responsibilities and identifying alternative solutions, while re-instating the positive impact of Secure Messaging on patients, healthcare providers and the healthcare sector.
Implementation	A misalignment of political agendas may result in ADHA being unable to effectively fulfil their responsibilities.	Medium <i>Rationale:</i> A misalignment of political agendas will inherently result in the delay or failure of key Secure Messaging initiatives.	Unlikely <i>Rationale:</i> Secure Messaging is one of the key strategic priority outcomes defined in the National Digital Health Strategy and the benefits are widely known and accepted.	Low	Facilitate leadership alignment sessions and resulting activities before further investment in the implementation of key initiatives.
Implementation	Vendors do not recognise the authority of the Governance group and choose to not participate.	High <i>Rationale:</i> Vendors provide the Secure Messaging software solution to end users. A lack of conformance activities will negatively impact the end user experience.	Possible <i>Rationale:</i> Vendors did not fulfil previous agreements.	High	Change and adoption initiatives to include consultation with vendors so that sentiments and concerns can be well understood.





Develop Secure Messaging Use Cases

Overview | Develop Secure Messaging Use Cases

This initiative aims to identify and document Minimum Viable Product Use Cases that can utilise the secure electronic exchange of clinical information between providers. This will provide an overview of the sender / receiver touchpoints, and will be used to enhance the end-to-end Secure Messaging process. Additionally, the Use Cases will be used to identify current barriers and would be used to develop recommendations for key initiatives.

Estimated Duration

6 months

Themes Addressed



Key Activities

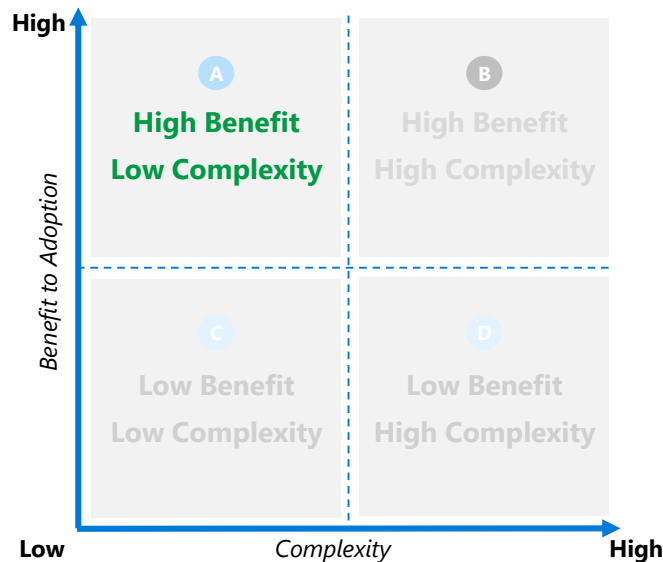
Key activities related to the development of Use Cases are (but not limited to):

- Identify stakeholders to be engaged and facilitate consultations
- Identify and prioritise (4-6) Use Cases to be developed and construct baseline scenarios
- Within each selected Use Case, understand the barriers for Secure Messaging usability
- Identify opportunities to implement Secure Messaging for each selected Use Case
- Gather Secure Messaging requirements for each Use Case
- Further refine and validate the Secure Messaging Use Cases
- Establish a repository for the storage of Secure Messaging Use Cases

Status

Not Started

Prioritisation Rating



This initiative was categorised as high benefit, as it will aid in tailoring the future program activities to each Use Case. This increases ease of usability of the Secure Messaging solution and directly impacts adoption rates. It is also categorised as low complexity, as baseline scenarios and Use Cases are already well understood and will require documentation and validation.



Stakeholder Impact | Develop Secure Messaging Use Cases

This initiative impacts three key stakeholder groups, namely ADHA, CIS and SMD vendors and end users.

Stakeholder Impact

Stakeholder	Impact	Explanation
ADHA	Neutral	ADHA will be responsible for identifying, documenting and evaluating Use Cases. Change and adoption activities will need to cater for the barriers and drivers identified while developing Use Cases.
CIS and SMD vendors	Negative	CIS and SMD vendors may need to customise their solutions based on the MVP Use Cases. This may require additional investment.
End users	Positive	The Secure Messaging solution will be customised to meet the requirements of the MVP Use Cases to enable end users to successfully utilise Secure Messaging.



Risk Assessment | Develop Secure Messaging Use Cases

Overall Initiative
Risk Rating:

Low

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Development	Use Cases do not holistically capture non-functional requirements of the end user (e.g. the need for a secure, reliable and fast internet connection, infrastructure, user experience, system behaviour and hardware requirements, training and support requirements etc.).	Medium <i>Rationale:</i> End users may acquire a working Secure Messaging solution, but do not have the external resources to support the use of the solution.	Unlikely <i>Rationale:</i> Non-functional requirements will vary case by case. The majority of end users already have a CIS or practice management / EMR system that is in use.	Low	Include non-functional requirements in the Use Cases.
Development	Use Cases take too much time to develop and delay initiatives that depend on them.	High <i>Rationale:</i> Due to varying environments and solutions used, Use Cases take too long to develop, validate and be approved. Thus, delaying program initiatives that depend on the specifics provided by Use Cases.	Unlikely <i>Rationale:</i> Key Use Cases have been identified and the next step is to document them.	Medium	Validate the timeline for Use Cases to be developed before documentation and consultation commences.
Development	Prioritised Use Cases do not reflect those which are pivotal for the success of the Program.	Medium <i>Rationale:</i> Incorrectly prioritised Use Cases may result in inappropriate specifications of initiatives that depend on it. Thus, specifications of roadmap initiatives may not meet their anticipated project outcomes.	Unlikely <i>Rationale:</i> Key Use Cases have been identified and the next step is to document them.	Low	Distribute the documented Use Cases among stakeholder working group and program governance before implementation.





*Agree on Secure Messaging
Standards and Develop a
Standards Framework
(in progress)*

Overview | Agree on Secure Messaging Standards and Develop a Standards Framework

This initiative aims to confirm the Secure Messaging Standards to be used across the end-to-end Secure Messaging process and develop a framework that will be mandated. The Standards Framework aims to provide guidance and conformance through a set of criteria for vendors to adhere to, and will be guided by selected Use Cases.

Estimated Duration

6 months

Themes Addressed



Key Activities

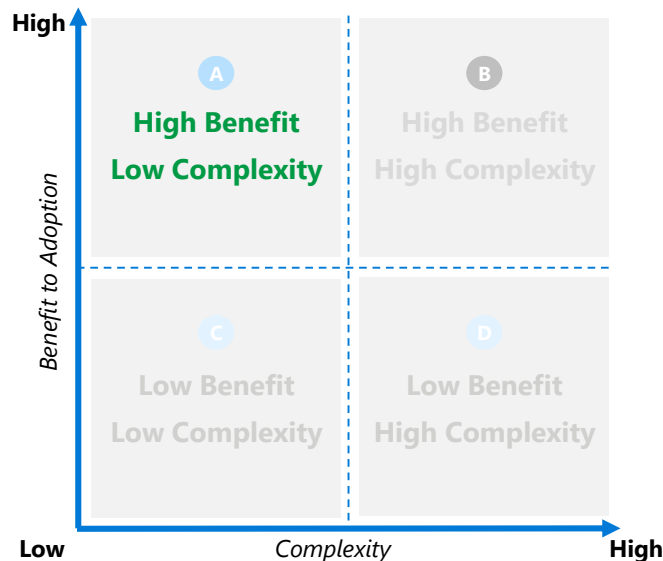
Key activities related to this initiative are (but not limited to):

- Establish a standards working group that involves ADHA stakeholders, vendor groups and external thought leaders
- Identify the standards and templates that are currently being used in the end-to-end Secure Messaging process
- Assess the standards against the requirements of the Use Cases
- Create a Standards Framework that address the conformity of the following:
 - Messaging payload standards
 - Implementation methodology of standards
 - Guidance on system behaviour and design
 - The use of directories and standards for searching
 - The use of PKI trust frameworks
 - Glossary of common terms and definitions
- Assess the overall impact to vendors and end users
- Establish an accreditation criteria and process that align with the Standards Framework
- Validate the Standards Framework with the working group
- Publish standards and Standards Framework

Status

PKI Trust Framework agreement is a work in progress

Prioritisation Rating



This initiative was categorised as high benefit, as it aims to provide guidance on the various factors that impact interoperability. Conformance to these standards directly influence the adoption rate of Secure Messaging. It is considered low complexity, as many of the components of the framework have been evaluated and are currently in progress.



Stakeholder Impact | Agree on Secure Messaging Standards and Develop a Standards Framework

This initiative impacts three key stakeholder groups, namely ADHA, CIS and SMD vendors and end users.

Stakeholder Impact

Stakeholder	Impact	Explanation
ADHA	Neutral	ADHA will act as the accreditor of CIS and SMD vendors. Additional processes and resources will be required to fulfil this responsibility.
CIS and SMD vendors	Negative	Vendors will be provided with a Standards Framework to support conformance and interoperability. Vendors will need to customise their products to meet the standards requirements.
End Users	Neutral	The Standards Framework will support interoperability and improve end user experience. Some end users may have to change their Secure Messaging solutions to those that are accredited according to the Standards Framework. This may result in a change in administrative processes.



Risk Assessment | Agree on Secure Messaging Standards and Develop a Standards Framework

Overall Initiative
Risk Rating:

Medium

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Development	Stakeholders who have input into the Standards Framework may not agree on the standards and it may take too long to develop.	High <i>Rationale:</i> Any initiative that is dependant on the completion of the Standards Framework will be delayed.	Likely <i>Rationale:</i> Some stakeholders may be required to invest more to customise their solution as a result of the Standards Framework.	High	Understand and acknowledge the strategic direction of impacted stakeholders as a result of the Standards Framework being completed (e.g. jurisdictions or vendors).
Development	Testing and accreditation processes do not cover the requirements stipulated by the Standards Framework.	High <i>Rationale:</i> If requirements set out in the Standards Framework are not covered, then the accreditation / testing process will not be effective.	Unlikely <i>Rationale:</i> The Standards Framework will inform the establishment of testing and accreditation processes.	Medium	Validate the alignment of the Standards Framework with the accreditation / testing processes.
Implementation	Standards may be interpreted and implemented differently by the various Secure Messaging vendors.	Medium <i>Rationale:</i> Different implementations of standards may result in inconsistent end user experiences and / or message templates.	Unlikely <i>Rationale:</i> Guidelines on the implementation of standards will be included in the Standards Framework.	Low	Provide vendors with a framework for implementation.
Implementation	Adoption may decrease due to vendors passing on development and customisation costs to end users, as a result of the implementation of the Standards Framework.	High <i>Rationale:</i> Costs of using Secure Messaging may outweigh the benefit realised, making the solution less attractive for end users. This may ultimately reduce adoption.	Possible <i>Rationale:</i> Technical interoperability impacts a Secure Messaging vendor's value proposition. This means that a vendor's margin is now dependent on customer fees.	High	When developing the Standards Framework, collaborate with vendors to support the alignment of their strategy to the vision of the Secure Messaging Program.





*Implement a Federated Secure
Messaging Directory Solution
(in progress)*

Overview | Implement a Federated Secure Messaging Directory Solution

This initiative aims to implement a Federated Secure Messaging Directory in order to consolidate healthcare provider directories from multiple sources. This allows for a federated directory that can be used by the end users to search a recipient healthcare provider's most up-to-date address.

Estimated Duration

In progress

Themes Addressed



Key Activities

Key activities related to this initiative are (but not limited to):

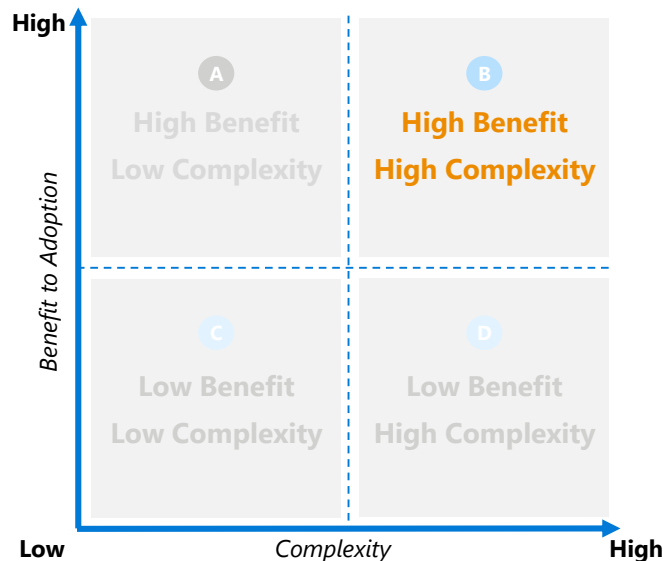
- Identify stakeholders to be engaged and facilitate consultations
- Understand and validate the current state challenges for implementing a Federated Secure Messaging Directory (including challenges around the use of the Service Registration Assistant)
- Assess alignment with the National Health Interoperability roadmap and identify gaps to be addressed
- Assess alignment with the Standards Framework
- Develop a data governance framework, in order to address data related challenges across the consolidation of directories
- Address identified gaps based on assessment against the National Interoperability roadmap and the Standards Framework
- Identify support and education requirements and incorporate into the Change and Adoption program
- Validate with stakeholders

Note: ADHA has currently invested in this initiative by establishing a Proof of Concept. One of the key vision statements of the National Health Interoperability roadmap focuses on the health service directory. Thus, ADHA may need to blend these two initiatives together in order to achieve greater interoperability.

Status

Implementation activities currently underway

Prioritisation Rating



This initiative was categorised as high benefit, as it increases the ease of use of the Secure Messaging solution and streamlines the end user experience. It is considered high complexity as it requires technical and business process changes.



Stakeholder Impact | Implement a Federated Secure Messaging Directory Solution

This initiative impacts three key stakeholder groups, namely ADHA, CIS and SMD vendors and end users.

Stakeholder Impact

Stakeholder	Impact	Explanation
ADHA	Neutral	ADHA is currently invested in this initiative and is responsible for the implementation of the Federated Secure Messaging Directory solution.
End Users	Positive	End users will have a single point to access provider information. This will result in a streamlined end user experience.
CIS and SMD vendors	Neutral	Vendors will need to adhere to data standardisation and governance requirements and confirm that their provider directories do not compromise data accuracy, completeness and integrity.



Risk Assessment | Implement a Federated Secure Messaging Directory Solution

Overall Initiative
Risk Rating:

High

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Implementation	The current Proof of Concept does not yield the expected benefits and hence no further investment is made.	High <i>Rationale:</i> End users will continue to experience current state challenges with regards to directories.	Unlikely <i>Rationale:</i> There is vested interest in this initiative and a willingness to address current challenges with directories.	Medium	Establish frequent checkpoints to track the alignment of the solution with expected outcomes.
Implementation	Directory providers do not implement the standardised API.	High <i>Rationale:</i> The Federated Secure Messaging solution will not be enabled.	Possible <i>Rationale:</i> Implementing a standardised API will require effort and investment by directory providers.	High	Proactively engage with directory providers to understand the effort or investment required.
Implementation	Directory providers do not allow access for searching their directories as required by the Federated Secure Messaging directory solution.	High <i>Rationale:</i> The Federated Secure Messaging solution will not be enabled.	Possible <i>Rationale:</i> Access to provider directories mean a loss of value proposition for the directory provider business.	High	The Standards Framework which will stipulate the use of directories and standards for searching, can be leveraged.





Establish a Change and Adoption Program

Overview | Establish a Change and Adoption Program

This initiative refers to a set of activities that address education, adoption and communication requirements across the Secure Messaging Program. The overarching goal is to assist all impacted stakeholders to transition into new behaviours and processes that support the success of Secure Messaging in Australia. Change and adoption activities will be tailored around selected Use Cases.

Estimated Duration

8 months

Themes Addressed



Key Activities

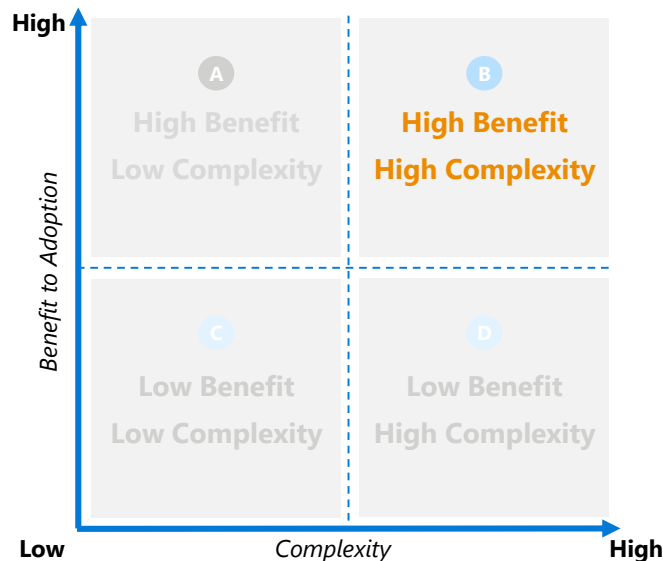
Key activities related to this initiative are (but not limited to):

- Facilitate the Secure Messaging Program leadership alignment consultations
- Develop a case for change with specific focus on moving away from manual workflows
- Identify and agree Change and Adoption approach
- Develop Change and National Scaling
- Develop Change and Adoption Implementation Plan based on agreed approach and strategy. This includes the following:
 - Develop a benefits realisation framework and plan
 - Identifying and documenting current Change and Adoption activities and analysing their effectiveness on increasing Secure Messaging adoption
 - Identifying key initiatives within the Program and the change they bring to the current Secure Messaging ecosystem
 - Identifying key stakeholder groups, developing a stakeholder map and conducting a Change Impact Assessment
 - Identifying Change and Adoption requirements and the resulting activities that fulfil those requirements
- Identify and engage Peak bodies, Local Health Services and Primary Health Network who will act as Change Champions and socialise the Change Implementation Plan

Status

General Secure Messaging education activities in progress

Prioritisation Rating



This initiative was categorised as high benefit, as it aims to increase Secure Messaging adoption rates through various tailored change and adoption activities. It is categorised as high complexity, as each activity will need to fully understand the barriers and drivers of selected Use Cases, and these vary from case to case.



Stakeholder Impact | Establish a Change and Adoption Program

This initiative impacts four key stakeholder groups, namely ADHA, Change Champions, CIS and SMD vendors and end user.

Stakeholder Impact

Stakeholder	Impact	Explanation
ADHA	Neutral	ADHA will need to have a dedicated team who are responsible for the design, development and implementation of the change and adoption activities.
Change Champions	Neutral	Change Champions will include SMD as a part of their agenda and support ADHA in delivering the outcomes of change and adoption activities.
CIS and SMD vendors	Positive	Vendors will be supported in the transition from current ways of working to those stipulated in the standards framework. They will also be given guidance on tools and methods for supporting and educating end users.
End Users	Positive	Change and adoption activities will support the education, support and communication of end users.



Risk Assessment | Establish a Change and Adoption Program

Overall Initiative
Risk Rating:

Medium

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Development	Use Cases are not fully understood and sufficiently fails to inform the Change and Adoption Program	High <i>Rationale:</i> The Change and Adoption program may not satisfy the requirements of the Use Cases.	Unlikely <i>Rationale:</i> The most prioritised Use Cases are well known throughout the industry	Medium	Validate the alignment of the Change and Adoption Program against the Use Cases
Implementation	Change Champions do not fulfil their responsibilities.	Low <i>Rationale:</i> If Change Champions are unable to fulfil their responsibilities, the communication channel between ADHA and end users will be impacted.	Unlikely <i>Rationale:</i> Change Champions are selected and approached based on their support to the success of Secure Messaging.	Low	Identify and recruit the right Change Champions and monitor their engagement over the activities.
Implementation	There is change fatigue among end users around the use of Secure Messaging.	High <i>Rationale:</i> Lack of participation of end users in change and adoption activities can drive down adoption rates and result in additional complexity introduced to the Secure Messaging Program	Unlikely <i>Rationale:</i> End users understand and appreciate the benefits of Secure Messaging and are generally keen to use the solution, as long as it works, reduces their administration burden and cost.	Medium	Confirm that interoperability is achieved and tested prior to change and adoption activities being implemented. Communicate successful case studies and highlight not only the financial benefit, but the benefit to the patient as well.





*Review NASH Process and
Develop a Suitable Trust
Framework
(in progress)*

Overview | Review NASH Processes and Develop a Suitable Trust Framework

This initiative aims to review current NASH processes and develop a suitable trust framework (such as a PKI Trust Framework) for healthcare providers who do not qualify for a NASH certificate. This will allow the acceptance of trusted certificates across the Secure Messaging Ecosystem.

Estimated Duration

In progress

Themes Addressed



Key Activities

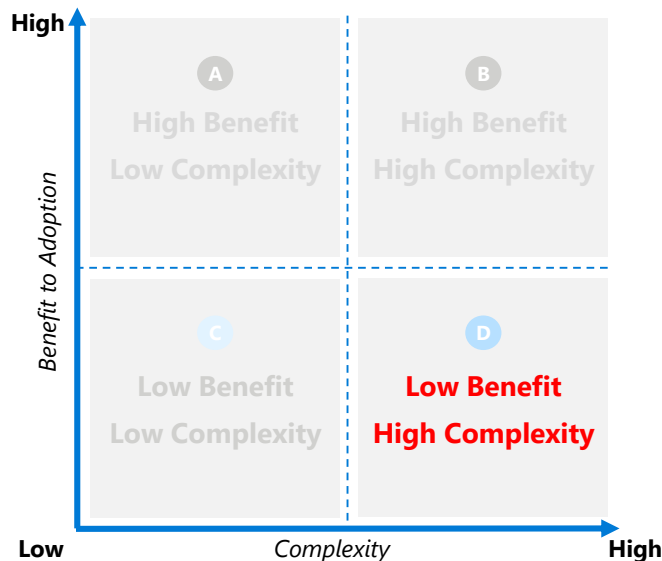
Key activities related to this initiative are (but not limited to):

- Review the current state of NASH process and identify opportunities for improvement (such as the automated updates of NASH certificates). *Note: The development of a trust framework is underway*
- Assess whether healthcare providers who have been identified through the Use Cases, align with NASH criteria
- Mandate the use of NASH certificates for those who are eligible
- Document requirements for healthcare providers who are not eligible for a NASH certificate
- Investigate frameworks (such as the Gatekeeper PKI framework or the DirectTrust framework) that are currently in use and assess fit-for-purpose for healthcare providers who are not eligible for a NASH certificate
- Develop a suitable trust framework for healthcare providers who are not eligible for a NASH certificate (i.e. individual healthcare providers registered in the HI Service and organisations such as Meals on Wheels)
- Identify areas of improvement and document steps to achieve them (e.g. automated installation of certificates)
- Develop an implementation plan

Status

Trust Framework activities currently underway

Prioritisation Rating



This initiative was categorised as low benefit, as NASH certificates are available to most end users. It is categorised as high complexity as healthcare providers that are not eligible for NASH certificates may have varying requirements that cannot be solved by a single solution.



Stakeholder Impact | Review NASH Processes and Develop a Suitable Trust Framework

This initiative impacts three key stakeholder groups, namely ADHA, CIS vendors and healthcare providers not eligible for NASH certificates.

Stakeholder Impact

Stakeholder	Impact	Explanation
ADHA	Neutral	ADHA will need to develop a trust framework for healthcare providers that are not eligible for NASH certificates.-ADHA will provide change and adoption support for the transition from current to future state processes.
SMD vendors	Negative	Vendors will need to trust each others PKI certificates, according to the requirements of the trust framework. As a result, there may be unforeseen security risks
Healthcare providers who are not eligible for NASH certificates	Positive	Healthcare providers or vendors who are not eligible for NASH will now have alternate framework to use. This will need to be incorporated into their current administrative processes to confirm that they can send messages securely.



Risk Assessment | Review NASH Processes and Develop a Suitable Trust Framework

Overall Initiative
Risk Rating:

Medium

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Development	Vendors, industry stakeholders and jurisdictions may not agree on a suitable trust framework	Medium <i>Rationale:</i> Current state challenges with PKI certificates (outside of NASH) will remain	Possible <i>Rationale:</i> Trust frameworks may not acknowledge all vendor, industry stakeholders and jurisdictional security requirements	Medium	The development of the trust framework should incorporate the requirements of secure data exchange policies, procedures and controls
Implementation	Once a suitable trust framework has been defined, organisations may not align or conform to the framework	Medium <i>Rationale:</i> Current state challenges with PKI certificates (outside of NASH) will remain	Possible <i>Rationale:</i> Participants may not adhere to the security and trust requirements outlined in the suitable trust framework	Medium	Establish quality assurance and security criteria that participants need to test against





*Develop a Secure Messaging
Lever Framework*

Overview | Develop a Secure Messaging Lever Framework

The Secure Messaging Lever Framework aims to increase end user adoption by expanding current healthcare processes to mandate the use of Secure Messaging. These processes include (but are not limited to) accreditation, professional standards, procurement and incentive schemes.

Estimated Duration

4 months

Key Activities

Key activities related to this initiative are (but not limited to):

- Identify levers in the industry. The following are a few examples (non-exhaustive):
 - General Practices*: RACGP to incorporate the use of an accredited Secure Messaging solution into the RACGP Standards for General Practices
 - Community Pharmacies*: The Pharmacy Guild of Australia to incorporate Secure Messaging into the Quality Care Community Pharmacy Standard; Pharmaceutical Society of Australia to incorporate Secure Messaging into the Professional Practice Standards
 - Pathology*: The National Pathology Accreditation Advisory Council to incorporate Secure Messaging into laboratory guidelines and standards
 - Diagnostic Imaging*: Diagnostic Imaging Accreditation Scheme (DIAS) Advisory Committee to amend the DIAS to incorporate the use of Secure Messaging
 - Hospitals*: Australian Committee on Safety and Quality in Health Care to incorporate Secure Messaging in the NSQHS Standards
 - Review of current incentive schemes used for Secure Messaging Adoption
- Develop a list of levers that can be leveraged for Secure Messaging
- Consult key stakeholders, Peak Bodies and accreditation councils
- Validate the framework through the governance processes
- Develop an implementation plan for amendment of selected professional standards and accreditations
- Build business case for each lever and secure funding as required

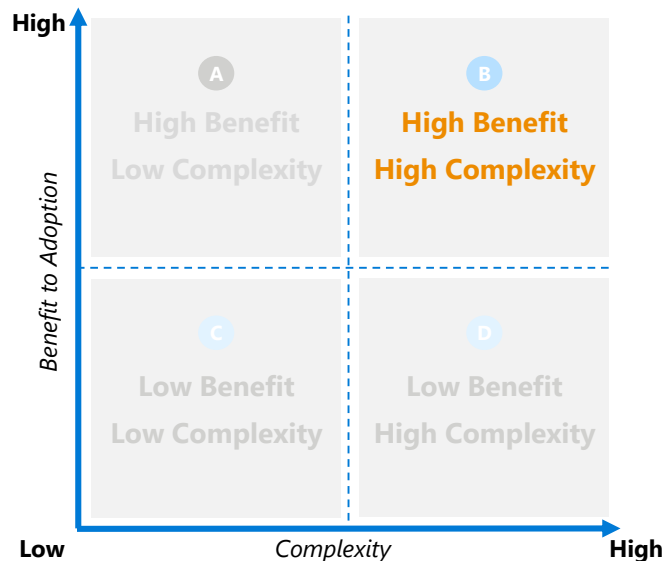
Status

Not Started

Themes Addressed



Prioritisation Rating



This initiative was categorised as high benefit, as it increases adoption of Secure Messaging through mandating it as a professional standard and accreditation requirement. It is considered high complexity as there are various professional standards and accreditation processes to be examined within each Use Case.



Stakeholder Impact | Develop a Secure Messaging Lever Framework

This initiative impacts three key stakeholder groups, namely Peak bodies and accreditation councils, ADHA and end users.

Stakeholder Impact

Stakeholder	Impact	Explanation
Peak bodies and accreditation councils	Neutral	Peak bodies and accreditation councils are responsible for amending current processes and communicating the changes to their respective communities of practice.
ADHA	Neutral	ADHA is responsible for identifying the correct stakeholder groups for consultation and ensuring that change and adoption activities articulate changes to current processes.
End Users	Neutral	End users will need to adopt Secure Messaging as a part of their practice management in order to remain compliant to professional standards and / or achieve professional accreditation.



Risk Assessment | Develop a Secure Messaging Lever Framework

Overall Initiative
Risk Rating:

High

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Development	Buy in for funding the changes to current incentive schemes, such as ePiP or MBS, (and the timeliness of implementation thereof) may not be achieved.	High <i>Rationale:</i> Changes to current incentive schemes will not be executed and may impact overall Secure Messaging adoption.	Possible <i>Rationale:</i> Incentive schemes have already been established and changing them will require additional review and effort.	High	A case for change needs to define a clear objective and articulate the expected benefits to increasing Secure Messaging adoption.
Development and Implementation	Buy in and conformance from accreditation and professional standards bodies may be difficult to achieve.	High <i>Rationale:</i> If the use of Secure Messaging is not timeously incorporated into accreditations and professional standards, target adoption rates may not be achieved.	Possible <i>Rationale:</i> Accreditation and professional standards bodies are currently not incentivised to explicitly include Secure Messaging in their accreditation and professional standards requirements.	High	Change and adoption initiatives should include the facilitation of conversations between DoH and Peak bodies to gain support and buy in.
Implementation	Force of habit by end users may result in the Lever Framework not achieving longevity of Secure Messaging adoption.	High <i>Rationale:</i> End users reverting back to paper based, manual transactions will not increase the adoption of Secure Messaging.	Unlikely <i>Rationale:</i> End users understand and appreciate the benefits of Secure Messaging and the solution.	Medium	Change and adoption initiatives should effectively promote the benefits of Secure Messaging. This can be done through showcasing success stories and Secure Messaging statistics. Additionally, investigate options to expand the criteria for claiming from benefit schemes or incentives. E.g. expanding requirement 2 of the ePiP eligibility criteria to include evidence of Secure Messaging volumes.





Establish an Innovation and Research Function

Note that this initiative is not included in the roadmap as it supports the wider National Digital Health Strategy and it is only included here as an optional initiative. However, there is applicability to the Secure Messaging program

Overview | Establish an Innovation and Research Function

The Innovation and Research function aims to support continuous improvement of secure, digital communication in healthcare. This will be through research and analysis of the global market and / or similar industries for process and solution improvements, as well as best practices that can be applied to the Australian market. This will also include exploring ideas and sentiments from various stakeholder groups within the broader interoperability agenda.

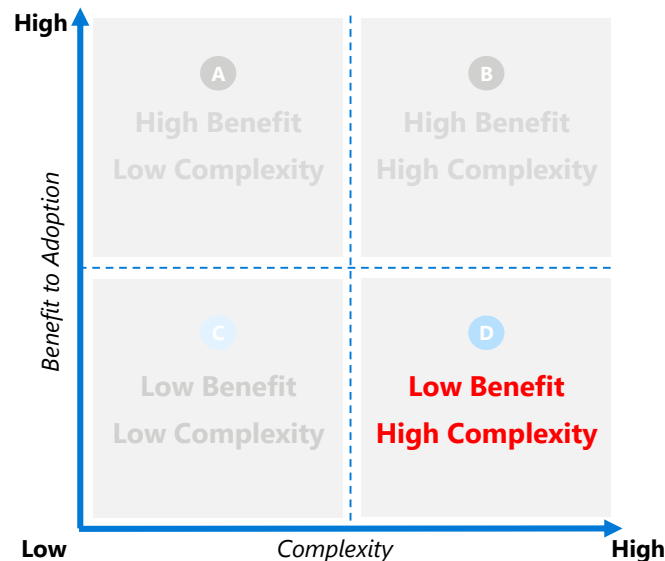
Estimated Duration

2 months

Themes Addressed



Prioritisation Rating



Key Activities

Key activities related to this initiative are (but not limited to):

- Develop the Innovation and Research function framework
- Develop the Innovation and Research strategy (with performance assessment indicators) and align with National Health Interoperability Roadmap vision and desired outcome
- Develop criteria for prioritising initiatives
- Develop the governance structure, roles, responsibilities and capabilities of the function
- Identify and prioritise the Innovation and Research initiatives and understand it's impact on the current Secure Messaging Ecosystem
- Potential areas of focus are as follows:
 - Impact of Cloud CIS
 - Possible integration into the My Health Record
 - Integration of patients and consumers into the Secure Messaging Ecosystem. e.g. patients being able to securely exchange messages with healthcare providers
 - Leveraging infrastructure from other sectors (e.g. Aged Care, Disability Sector, Emergency Services and Prison Services) in order to readily exchange information

Status

Not Started

This initiative was categorised as low benefit, as it does not directly impact the adoption rate of Secure Messaging, but rather focuses on new technologies and solutions for secure, digital communication within healthcare. It was categorised as high complexity, as it will be incorporated into the interoperability agenda and covers a vast amount of Use Cases and requirements.



Stakeholder Impact | Establish an Innovation and Research Function

This initiative impacts four key stakeholder groups, namely ADHA, CIS and SMD vendors, end users and Peak bodies, professional standards and accreditation councils.

Stakeholder Impact

Stakeholder	Impact	Explanation
ADHA	Neutral	ADHA will be responsible for portfolio and business case management, and will be involved in the implementation and management of resulting programs.
CIS and SMD vendors	Negative	The value proposition of CIS and SMD vendors may be compromised, depending on the nature of new technologies and solutions.
End Users	Negative	End users may be required to invest in new technologies and solutions as the secure, digital communication market shifts. This may also require a change in ways of working.
Peak bodies, professional standards and accreditation councils	Negative	Professional standards and accreditations that specifically mandate the use of Secure Messaging will need to be amended to adhere to changes in the solution.



Risk Assessment | Establish an Innovation and Research Function

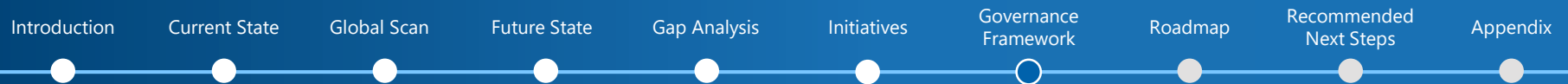
Overall Initiative
Risk Rating:

High

Risk Type	Risk Description	Risk Impact	Risk Likelihood	Risk Rating	Mitigating Action
Implementation	The Innovation and Research function may identify new technology solutions for the secure exchange of clinical information. This may impact the current Secure Messaging Program initiatives.	High <i>Rationale:</i> Initiatives and activities of the function may need to be re-designed.	Possible <i>Rationale:</i> The rapid evolution of technology means that there will be new opportunities and solutions for the secure exchange of clinical information and data.	High	Evaluate new options for the secure exchange of clinical information and develop a sustained transition roadmap that best leverages the current investments made in Secure Messaging.



Governance Framework



The Governance Framework aims to support the vision of the Secure Messaging Program and is realised by providing clear roles, responsibilities and guidelines

There are multiple CIS vendors and SMD vendors currently in the market. One of the key challenges faced by vendors is the lack of guidance on and conformance to message format templates. In addition, participation by the broader vendor group has been low as conformance has not been mandatory. As a result, these vendors have only been able to achieve pockets of success across Australia.

The Secure Messaging Governance Framework aims to provide direction and control through a set of roles and responsibilities, activities and stakeholder interactions. The framework will be used to support and maintain the oversight and management of all contributing factors of the Secure Messaging Program.

The governance framework supports the delivery of the vision of the Secure Messaging Program and is realised by:



Outlining the organisational structure of the key stakeholder groups involved



Clearly defining the roles and responsibilities of each stakeholder group



Ensuring that Standards and Lever Frameworks are defined, understood and adhered to



Provide a reporting mechanism that will be used for performance monitoring, decision making and continuous improvement initiatives



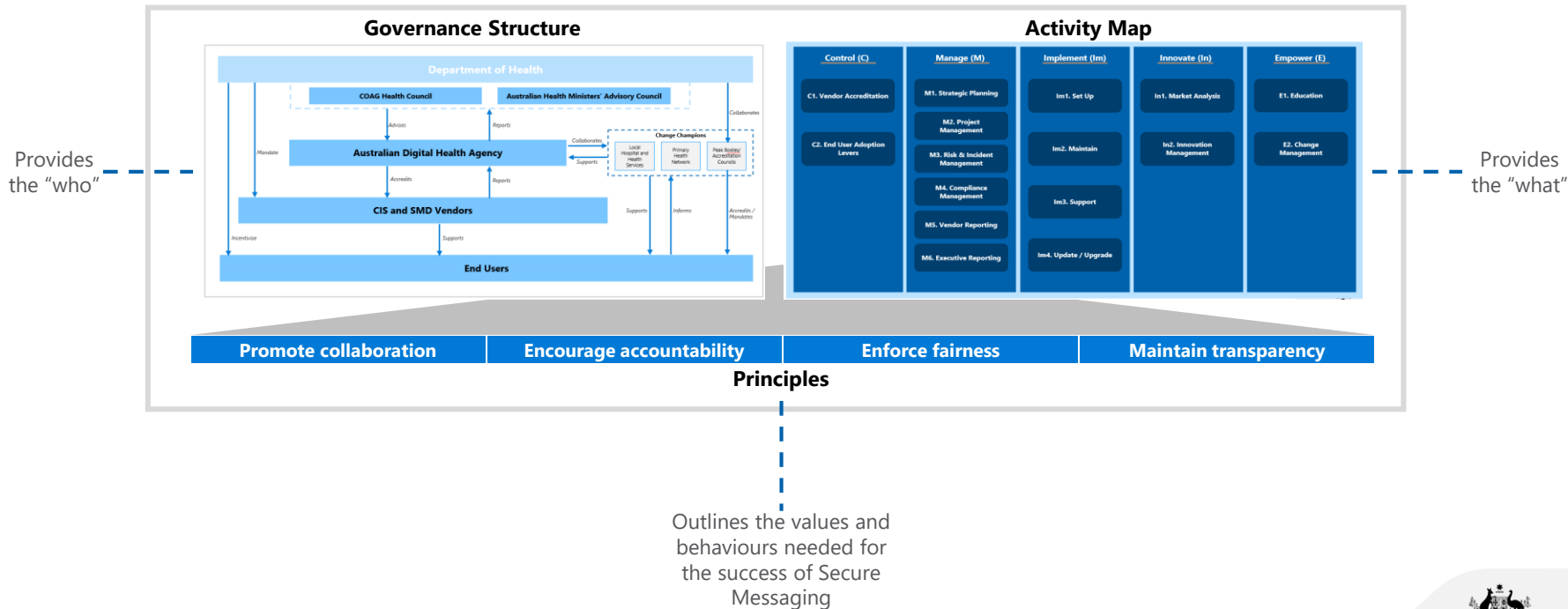
Ensuring accountability and quality of service through defined KPIs



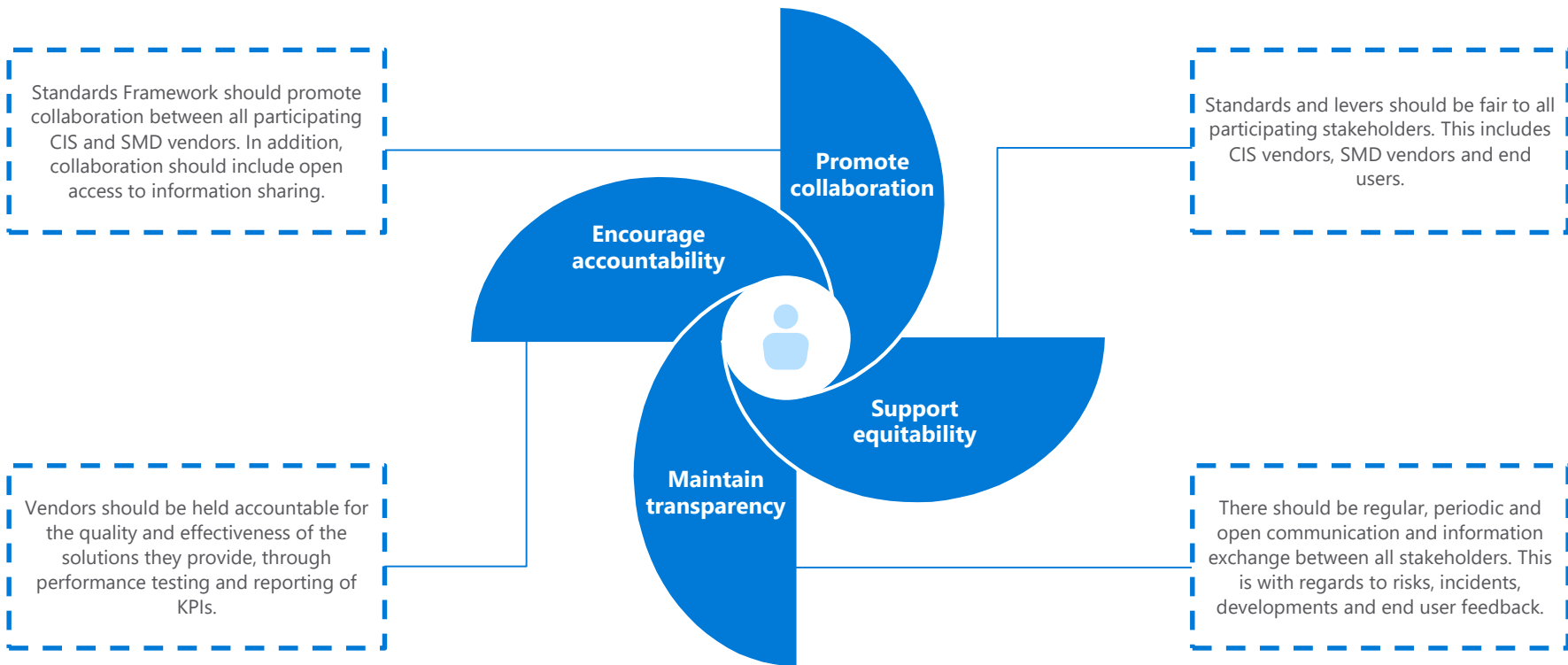
Providing a clear risk and incident management process

The Governance Framework is comprised of three components: the Governance Structure and corresponding Activity Map, which is underpinned by the Governance Principles

Components of the Governance Framework:

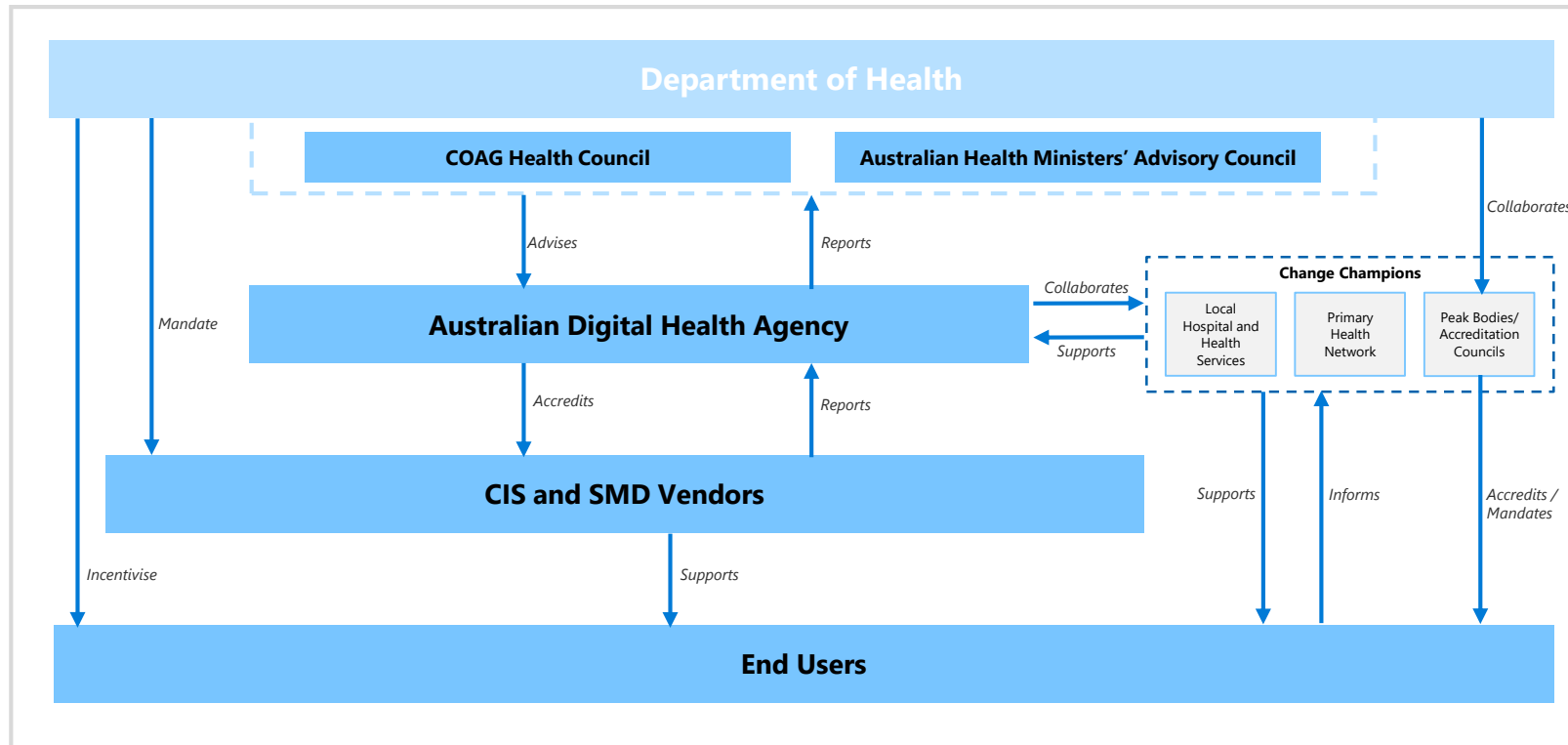


The Governance Framework Principles provides a foundation for the behaviours that promote the success of Secure Messaging Adoption in Australia



Each principle is centred around what is best for the end user experience and ultimately the patient.

The Governance Structure highlights all the key stakeholders and interactions that support the Secure Messaging Program and it's initiatives



Each stakeholder group has specific roles and responsibilities that support the success of the Secure Messaging Ecosystem (1/2)

Department of Health

The Department of Health (DoH) acts as the **control body** for the Secure Messaging Program. It is the **highest** point of **decision making**. The DoH is responsible for mandating the following:

- The Standards Framework for CIS and SMD vendors
- Temporary transaction-based, per-message incentive schemes for end users

In addition, the DoH is responsible for collaborating with Peak bodies and accreditation councils on the inclusion of Secure Messaging in health practitioner accreditations and professional standards (in accordance with the Levers Framework).

The DoH advises the Australian Digital Health Agency through the COAG Health Council and **Australian Health Ministers' Advisory Council**.

Australian Digital Health Agency

The Australian Digital Health Agency (ADHA) will play a **lead management role** within the Secure Messaging Program. The responsibilities of ADHA can be summarised as follows:

- Day-to-day co-ordination of implementation and engagement activities, as well as long term strategic planning (or **program management**)
- Develop the Standards Framework
- Lead the Change and Adoption Program
- Accredit vendors in conformance to the Standards Framework
- Develop the Secure Messaging Lever Framework
- Facilitate discussions with regard to **continuous improvement** and **innovation**
- Collaboration with Change Champions to implement and **promote change** and **adoption activities**.

COAG Health Council and Australian Health Ministers' Advisory Council

The COAG Health Council (CHC) and its advisory body, the Australian Health Ministers' Advisory Council (AHMAC) play the role of an **intermediary forum** to **discuss performance, risks, issues** and **developments** within the Secure Messaging Program. CHC and AHMAC advise on behalf of DoH and provide a forum that supports state and territory governments. The responsibilities of CHC and AHMAC can be summarised as follows:

- Provide **guidance** and **support** to the **ADHA** with decisions in relation to **programme activities** and **funding**
- **Advise** on the development of the **Standards Framework**

Change Champions

Change Champions include **local health services**, the **Primary Health Networks**, **Peak bodies** and accreditation councils. They will collaborate with **ADHA** and **end users** and will act as drivers for change and adoption in the industry. The responsibilities of Change Champions can be summarised as follows:

- Being an **active part** of the development and implementation of **adoption** and **education programmes**
- **Promoting** the **implementation** and **adoption** of Secure Messaging and **communicating** its **benefits** to end users
- Supporting ADHA in **continuous improvement** and **innovation** around the Secure Messaging Program.

Peak bodies and accreditation councils are responsible for mandating the use of Secure Messaging as an accreditation and professional standards requirement.



Each stakeholder group has specific roles and responsibilities that supports the success of the Secure Messaging Ecosystem (2/2)

Clinical Information System Vendors

The Clinical Information System (CIS) vendors provide the **software solution** that is used by **end users**. Their responsibilities can be summarised as follows:

- **Maintaining interoperability** with **Secure Messaging vendors** and supports a **seamless experience** for end users
- Confirm that **end users receive the support and education** they need with regards to the software solution
- Maintaining a high quality service through **diligent reporting** to the ADHA and Secure Messaging vendors.
- Confirm that software products **adhere** to **conformance requirements** as outlined in the **Standards Framework**.

End Users

End users are imperative to the success of Secure Messaging Adoption. Given the current Secure Messaging Ecosystem, the vast majority of end users are **healthcare providers** and have the responsibility to **invest in** and **use Secure Messaging** solutions. They are also responsible for **communicating concerns, ideas** or process improvement **suggestions** to ADHA via the Change Champions, and ensuring that their healthcare practice adheres to the Secure Messaging requirements as outlined in professional standards and accreditations.

SMD Vendors

The Secure Messaging vendors provide the **interconnection solution** that **interfaces** with a sender and receiver **CIS software solution** (or end point). Their responsibilities can be summarised as follows:

- Maintaining a **secure, interoperable link** with other SMD vendors and CIS vendors
- Ensuring a **seamless experience** for CIS vendors and end users through **support** and **training** as required
- Maintaining a **high quality service** through **reporting** to the ADHA and CIS vendors
- Confirm that software products **adhere** to **conformance requirements** as outlined in the **Standards Framework**.



Introduction Current State Global Scan Future State Gap Analysis Initiatives Governance Framework Roadmap Recommended Next Steps Appendix

The Activity Map provides a snapshot view of all key activities required to sustain a successful Secure Messaging Program, and is comprised of five activity groups

Control (C)

These activities include developing and mandating frameworks that provide guidance on technical standards, deadlines and selected adoption levers.

Manage (M)

These include the day-to-day co-ordination of implementation and engagement activities, as well as long term strategic planning (or program management), as well as compliance management activities.

Implement (Im)

These activities include the execution of the Secure Messaging systems and technical workflows between CIS and SMD vendors.

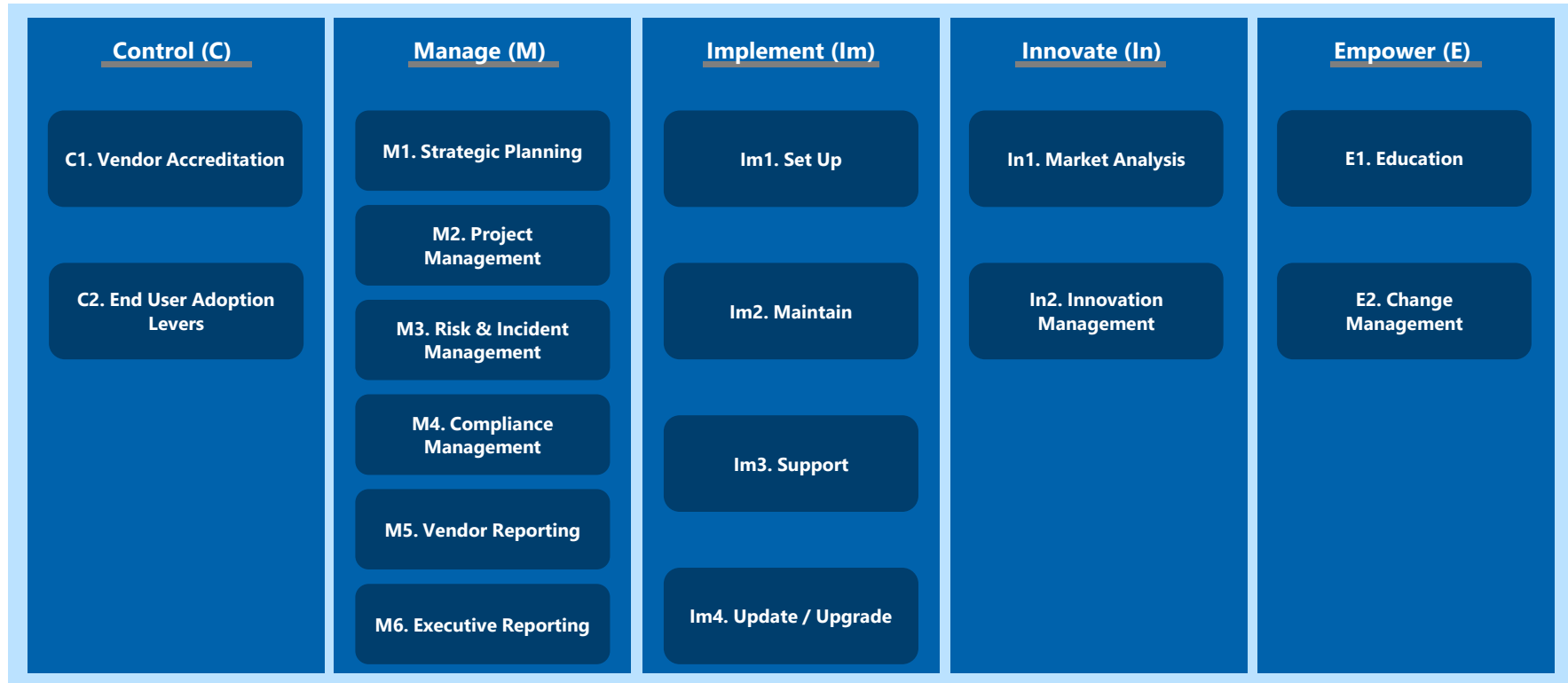
Innovate (In)

These activities includes continuous improvement discussions and initiatives.

Empower (E)

These activities are those that promote change and adoption among end users.

Each activity group of the Activity Map is further broken down into key sub-activities



The following tables detail the key activities within the “Control” activity group of the Secure Messaging Program

Item	C1. Vendor Accreditation
Objective	To develop, mandate and accredit against the Standards Framework that provides guidance and conformance through a set of criteria that CIS and SMD vendors are to adhere to. The Standards Framework aims to encourage standardisation and interoperability across the Australian healthcare industry.
Input	Selected Use Cases, technical requirements analysis, messaging guidelines and templates.
Output	The Standards Framework and its mandate.
Timing	TBD.
Responsibility	It is the responsibility of ADHA to develop the Standards Framework and accredit vendors in accordance to the criteria stipulated in the framework. The DoH is responsible for mandating the Standards Framework to vendors.
High Level Activities	Refer to high level activities stated in the ‘Agree on Secure Messaging Standards and Develop a Standards Framework’ overview slide
Decisions	The selected messaging standards and templates need to support the highest level of interoperability with the least amount of industry disruption and investment. A deadline for interoperability needs to be stipulated.
Item	C2. End User Adoption Levers
Objective	To encourage Secure Messaging adoption by incorporating the use of Secure Messaging in healthcare practitioner accreditation and professional standards, as well as other incentive schemes.
Input	Use case analysis, stakeholder consultation and industry research.
Output	The Secure Messaging Lever Framework and its mandate.
Timing	TBD
Responsibility	It is ADHA’s responsibility to develop the Secure Messaging Lever Framework, while the DoH will mandate the framework to Peak Bodies and accreditation councils. The appropriate Peak Body or accreditation council will be responsible for incorporating Secure Messaging into accreditations and professional standards. It is the responsibility of the DoH to fund end user incentive schemes.
High Level Activities	Refer to high level activities stated in the ‘Develop a Secure Messaging Lever Framework’ overview slide
Decisions	The Secure Messaging Lever Framework needs to provide a list of accredited vendors that healthcare providers can select from.



The following tables detail the key activities within the “Manage” activity group of the Secure Messaging Program (1/3)

Item	M1. Strategic Planning
Objective	To define the strategic direction for a given period of time. This includes identifying projects or initiatives that support the adoption or improvement of Secure Messaging and their order of execution.
Input	Secure Messaging vision and strategy and stakeholder consultation.
Output	Program implementation plan, resource plan, budget allocation.
Timing	At the beginning of each major project / initiative.
Responsibility	Strategic planning is the responsibility of the ADHA, with guidance from the COAG and AHMAC.
High Level Activities	<ul style="list-style-type: none"> Confirm vision and end goals Develop execution plan Develop stakeholder and communication plan Implement and monitor execution plan
Decisions	Plan should identify resources required, allocate time realistically and involve engagement of the right stakeholder groups.

Item	M2. Project Management
Objective	To support the Secure Messaging program and its related projects / initiatives realise its vision and milestones.
Input	Stakeholder consultations and decisions, requirements analysis, implementation plans, stakeholder engagement maps and plans, communication plans, budget plans.
Output	Dependant on particular project or initiative.
Timing	Dependant on particular project or initiative.
Responsibility	It is the responsibility of ADHA to facilitate and co-ordinate project management activities and develop project management outcomes.
High Level Activities	<p>Specific activities will depend on the project or initiative.</p> <p>However, each project or initiative will include baselining exercises to track and record benefits over time.</p>
Decisions	Dependant on particular project or initiative.



The following tables detail the key activities within the “Manage” activity group of the Secure Messaging Program (2/3)

Item	M3. Risk & Incident Management
Objective	To develop control plans for potential negative occurrences and the development and execution of control plans for negative occurrences that have already transpired.
Input	Risk and incident management framework, policies and procedures.
Output	Risk management report, incident management report and post-incident plan.
Timing	Ad-hoc.
Responsibility	It is the responsibility of the ADHA to report on risks and incidents. It is the responsibility of the CHC and AHMAC to provide guidance and support with mitigating activities.
High Level Activities	<ul style="list-style-type: none"> Analyse risk or incident Evaluate impact on Secure Messaging Ecosystem Develop mitigating actions with key stakeholders Execute mitigating actions (if incident occurred) Develop risk / incident management report
Decisions	Dependent on nature of risk or incident.
Item	M4. Compliance Management
Objective	To monitor compliance and performance of vendors, in according to the requirements of the Standards Framework. Inherently, to determine the success of interoperability across the Ecosystem.
Input	The Standards Framework
Output	Compliance reports.
Timing	Annual compliance testing.
Responsibility	It is the responsibility of the ADHA to perform compliance management activities and the responsibility of the Secure Messaging to perform internal compliance checks to confirm that their software products adhere to the requirements stipulated in the Standards Framework.
High Level Activities	<ul style="list-style-type: none"> Develop compliance management plan, including milestones and reporting cadence Perform compliance management activities against requirements stipulated in the Standards Framework Develop compliance reports and key actions Review and update plan accordingly
Decisions	Vendors who are not compliant to the Standards Framework will not be provided a Secure Messaging accreditation.



The following tables detail the key activities within the “Manage” activity group of the Secure Messaging Program (3/3)

Item	M5. Vendor Reporting
Objective	To support transparency of performance of the Secure Messaging solution and encourage the highest quality service to end users.
Input	Performance reporting templates and vendor KPIs
Output	Vendor Performance Report and Annual Compliance Testing Report
Timing	Quarterly and annually for compliance testing
Responsibility	It is the responsibility of the SMD vendors to submit performance reports to the ADHA on a monthly basis and to submit their annual compliance testing report annually. Reporting between SMD and CIS vendors may occur within their own terms.
High Level Activities	<ul style="list-style-type: none"> Collect performance metrics Complete reporting template Submit monthly performance reporting, as well as annual compliance report to ADHA
Decisions	Content of reports should be accurate and quantifiable.

Item	M6. Executive Reporting
Objective	Support transparency of the performance or success of the Secure Messaging Program to CHC and AHMAC, and showcase conformance to mandated frameworks.
Input	Executive reporting templates, vendor KPIs, program status summary.
Output	Executive Report., which includes an overall program status update, risks and issues (with mitigating activities) , new developments and market changes.
Timing	Quarterly.
Responsibility	The ADHA is responsible for the development and submission of the Executive Report. CHC and AHMAC are responsible for making key decisions.
High Level Activities	<ul style="list-style-type: none"> Consolidate vendor reports into key insights Develop Executive Report Submit Executive Report Action any activities required by COAG and AHMAC
Decisions	Executive report(s) should outline the status of the Secure Message Program, nationally.



The following tables detail the key activities within the “Implement” activity group of the Secure Messaging Program (1/2)

Item	Im1. Set up
Objective	To confirm that the technical and clinical requirements of the end user are met, CIS and SMD solutions are interoperable and that healthcare messages are transmitted securely and seamlessly.
Input	End user requirements, clinical workflows technical standards and templates.
Output	Requirements specification and agreed standards.
Timing	TBD
Responsibility	It is the responsibility of the SMD and CIS vendors to confirm that the end user is provided with a working solution and can communicate with all end points.
High Level Activities	<ul style="list-style-type: none"> Identify and document specific end user requirements Install Secure Messaging software Perform system integration testing to confirm that data flow between software interfaces is seamless
Decisions	The end user interface needs to be seamless and easy to use. Secure Messaging software needs to integrate with CIS solution using the technical standards.

Item	Im2. Maintain
Objective	To confirm that the end user has a constant and effective Secure Messaging solution, the solution operates within the agreed technical standards and all service interruptions are managed.
Input	Incident management, problem management, event management, service request fulfilment and access management reporting templates, software maintenance plans.
Output	Completed incident management, problem management, event management, service request fulfilment and access management reports, end user guides.
Timing	Ongoing.
Responsibility	It is the responsibility of the Secure Messaging vendors to confirm that all maintenance activities are performed and there are minimal service interruptions.
High Level Activities	<ul style="list-style-type: none"> Perform and document incident management activities Perform and document problem management Perform and document event management Facilitate service request fulfilment Perform and document access management Perform and document event management
Decisions	Decisions are based on type of incident, problem, event and service request.



The following tables detail the key activities within the “Implement” activity group of the Secure Messaging Program (2/2)

Item	Im3. Support
Objective	To increase adoption of Secure Messaging by ensuring that the end user is provided with the education and support they need to use the solution.
Input	Training manuals and other education materials.
Output	Customised end user support material, as required by end user.
Timing	As required.
Responsibility	It is the responsibility of the Secure Messaging and CIS vendors to provide the technical support required by end users.
High Level Activities	<ul style="list-style-type: none"> Investigate user challenges / requirements Identify possible solutions Implement solutions Develop post-support reports as required
Decisions	Decisions are based on the support request.
Item	Im4. Update / Upgrade
Objective	To support a seamless end user experience and interoperability by when software is updated or upgraded with latest features and capabilities.
Input	Software update / upgrade requirements, testing plans, change control plans, compliance guidelines.
Output	Update / upgrade review documentation, end user training guides.
Timing	As updates / upgrades occur.
Responsibility	It is the responsibility of the SMD and CIS vendors to confirm that software updates are implemented successfully and interoperability is maintained.
High Level Activities	<ul style="list-style-type: none"> Review current solution and undertake change control planning Establish update / upgrade requirements Develop an update / upgrade plan (including backup plan) Run a trial update / upgrade Perform testing (functional, non-functional and technical testing, technical standard compliance, data integrity, security and performance testing) Undertake configuration Provide training and support to end users, as required Perform an update / upgrade review
Decisions	Software updates should cause limited disruption of practice operations and should have a limited number of changes to user experience.



Introduction Current State Global Scan Future State Gap Analysis Initiatives Governance Framework Roadmap Recommended Next Steps Appendix

The following tables detail the key activities within the “Innovate” activity group of the Secure Messaging Program

Item	In1. Market Analysis
Objective	To scan the global market and / or similar industries for process and solution improvements, as well as best practices that can be applied to the Australian market.
Input	N/A
Output	Market analysis report and findings.
Timing	Half yearly.
Responsibility	It is the responsibility of the ADHA to perform market analysis and to develop a market analysis report on a quarterly basis.
High Level Activities	<ul style="list-style-type: none"> • Conduct research on mature markets and identify what works and what doesn't work • Engage with key stakeholders to understand sentiments or new developments in the market • Document findings and relevance to Australian market
Decisions	The market analysis activity should be conducted with the aim of improving the Secure Messaging Program.
Item	In2. Innovation Management
Objective	To gather, collate, investigate ideas and sentiments from various stakeholder groups within the Secure Messaging Program, and facilitate conversations in relation to innovation and improvement.
Input	Suggestions, ideas and sentiments of stakeholders within the Secure Messaging Program.
Output	Shortlisted set of initiatives to be included on an optimisation roadmap.
Timing	Quarterly, in conjunction with the market analysis report.
Responsibility	It is the responsibility of the ADHA to gather, collate and investigate suggestions, ideas and sentiments, facilitate further discussions and develop initiatives.
High Level Activities	<ul style="list-style-type: none"> • Gather feedback from stakeholders (e.g. Peak Bodies, SMD and CIS vendors, Primary Health Network etc.) • Investigate feedback and facilitate further discussion if needed • Develop a report of selected initiatives and findings
Decisions	Feedback that is taken up as an initiative needs to be fair and aimed at finding opportunities for improvement within the Secure Messaging Program.



The following tables detail the key activities within the “Empower” activity group of the Secure Messaging Program

Item	E1. Educate
Objective	To accelerate change and adoption by educating healthcare providers on the benefits of using Secure Messaging.
Input	Education program plans.
Output	Secure Messaging education roadshows, education material, seminars etc.
Timing	Timing depends on education program plans.
Responsibility	It is the responsibility of the ADHA to develop education program plans and work with Change Champions to roll out the plan.
High Level Activities	<ul style="list-style-type: none"> Identify all stakeholders to be targeted by the education program Develop education program plan Provide materials and access for education Roll out education program plan
Decisions	Education initiatives need to consider all types of stakeholders and their preferred channel of education and communication.

Item	E2. Change Management
Objective	In conjunction with the education programme, change management supports stakeholders in being prepared for the transition to Secure Messaging (if the solution is not already being used).
Input	Stakeholder and impact analysis.
Output	Change management initiatives and plan.
Timing	Timing depends on the change management plan.
Responsibility	It is the responsibility of the ADHA to develop the change management plan and work with Change Champions to confirm that the plan is implemented effectively and efficiently.
High Level Activities	Activities will be determined by the Change and Adoption Program at a single point in time.
Decisions	The initiatives on the change management plan should be end user centred.



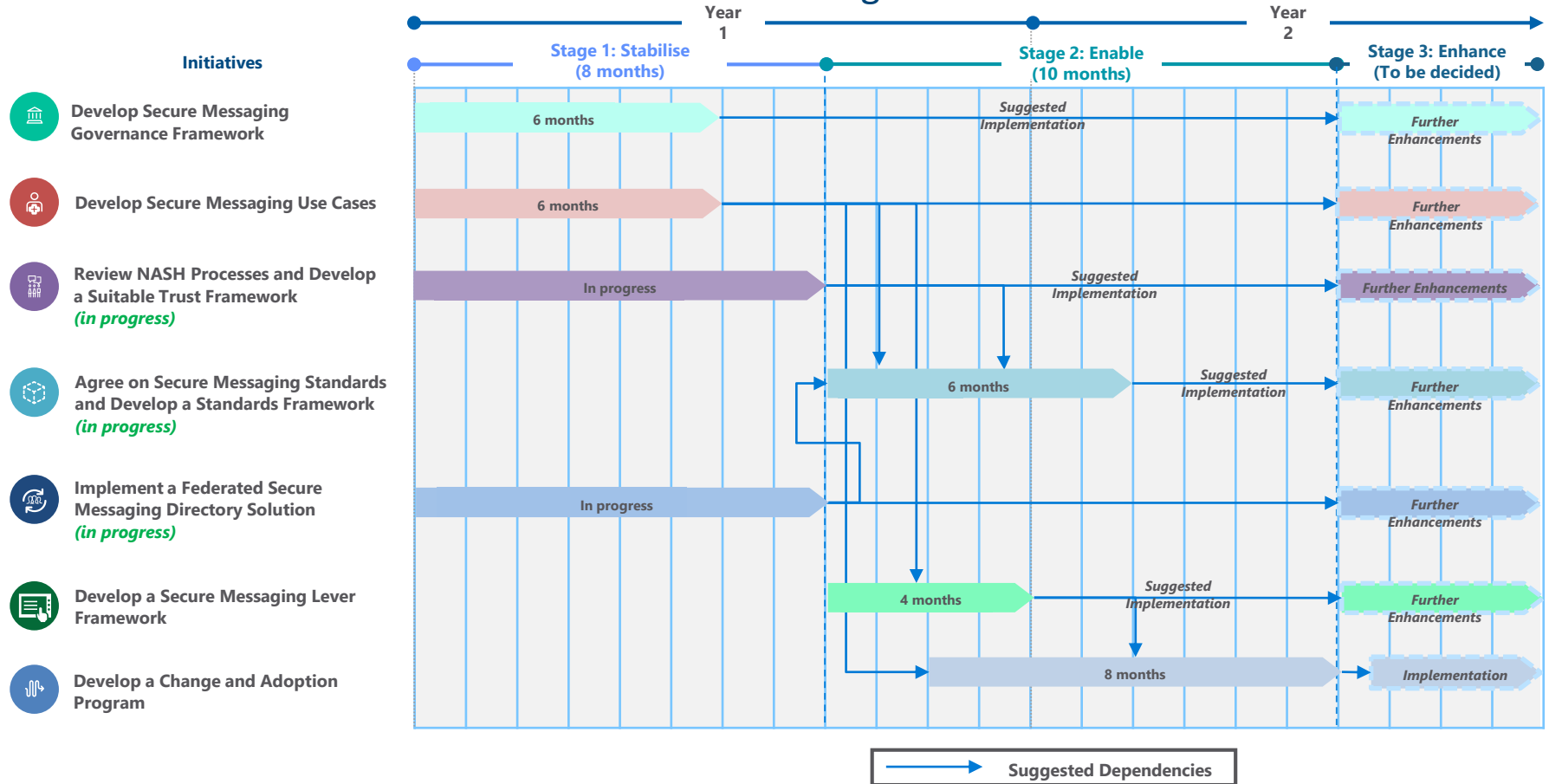
Roadmap



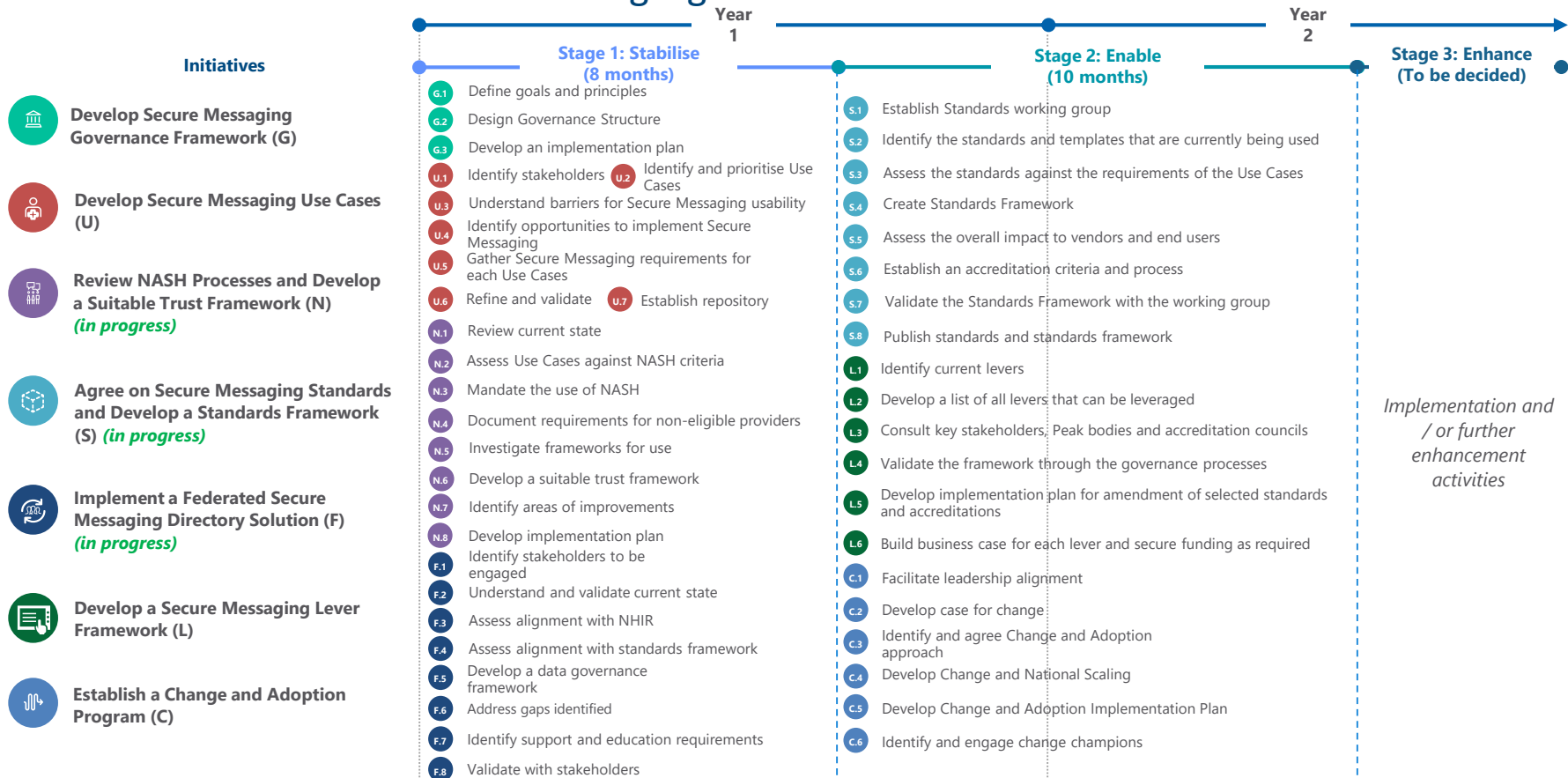
The proposed roadmap categorises activities into three enabling stages, namely “Stabilise”, “Enable” and “Enhance”



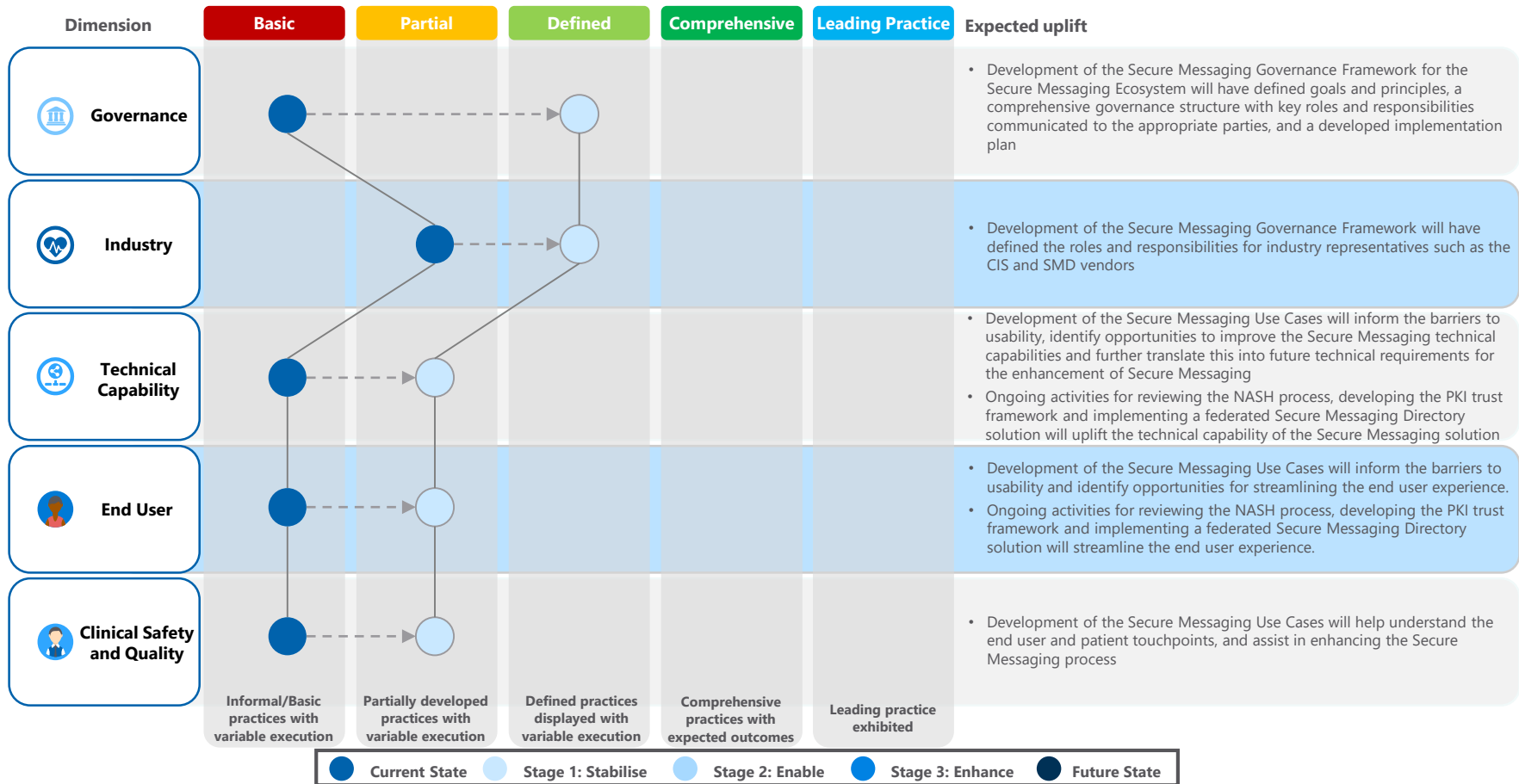
The seven key initiatives aim to be delivered over a two year roadmap, that will be divided into the three stages



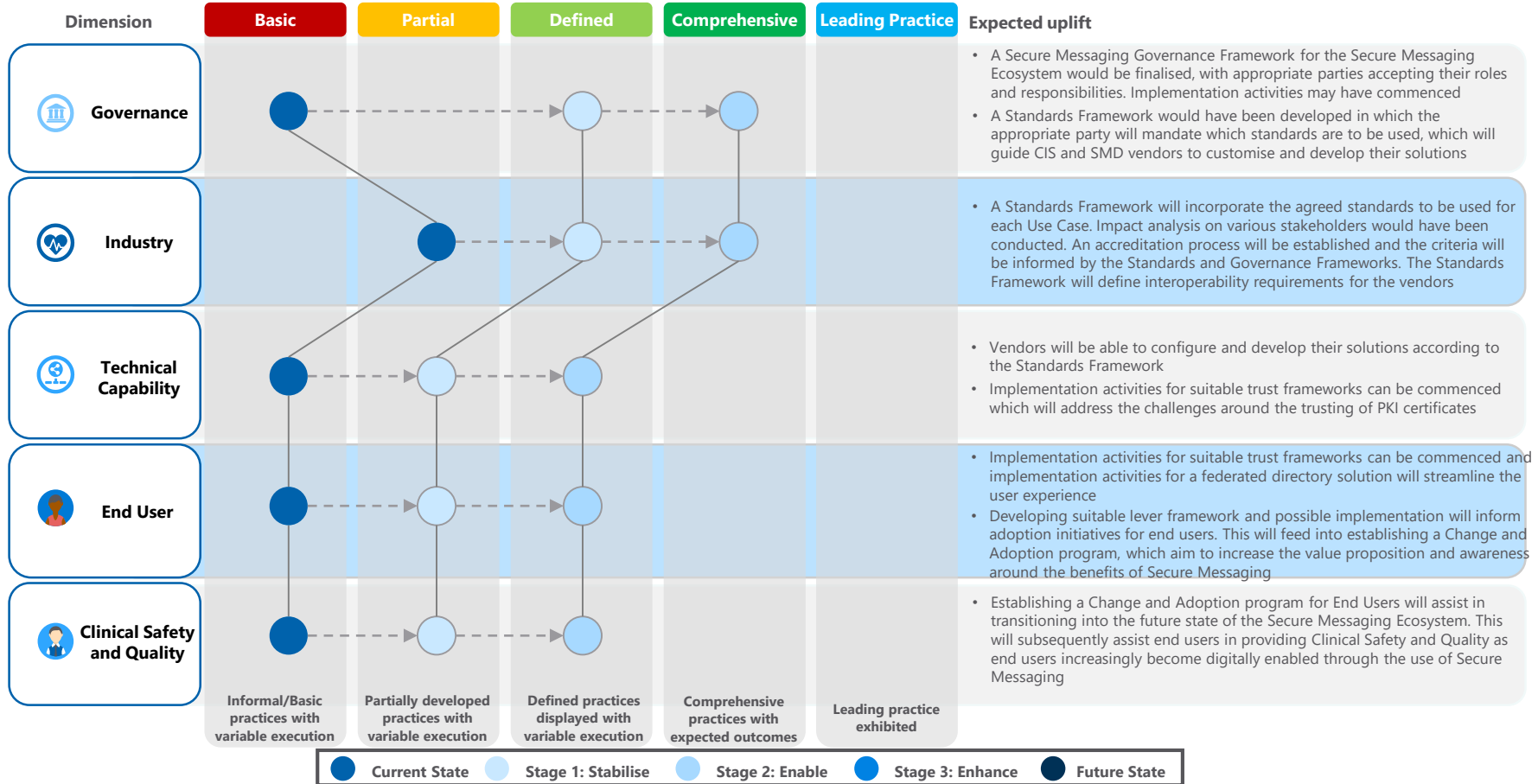
The seven key initiatives aim to be delivered over a two year roadmap and contain the following high level “bodies of work”



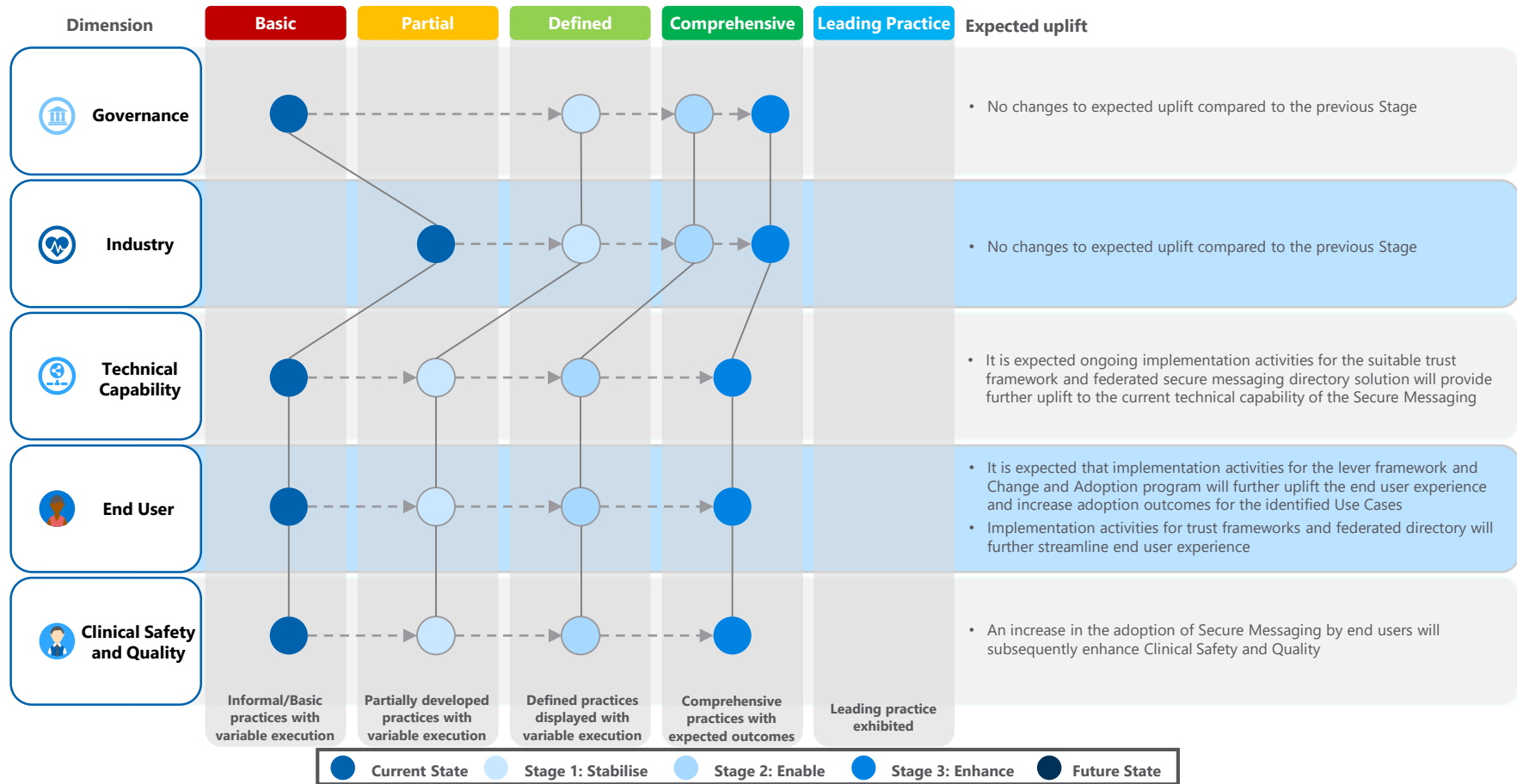
Stage 1: Stabilise phase will focus on initiatives that aim to lay the foundation for control, oversight, interoperability and collaboration



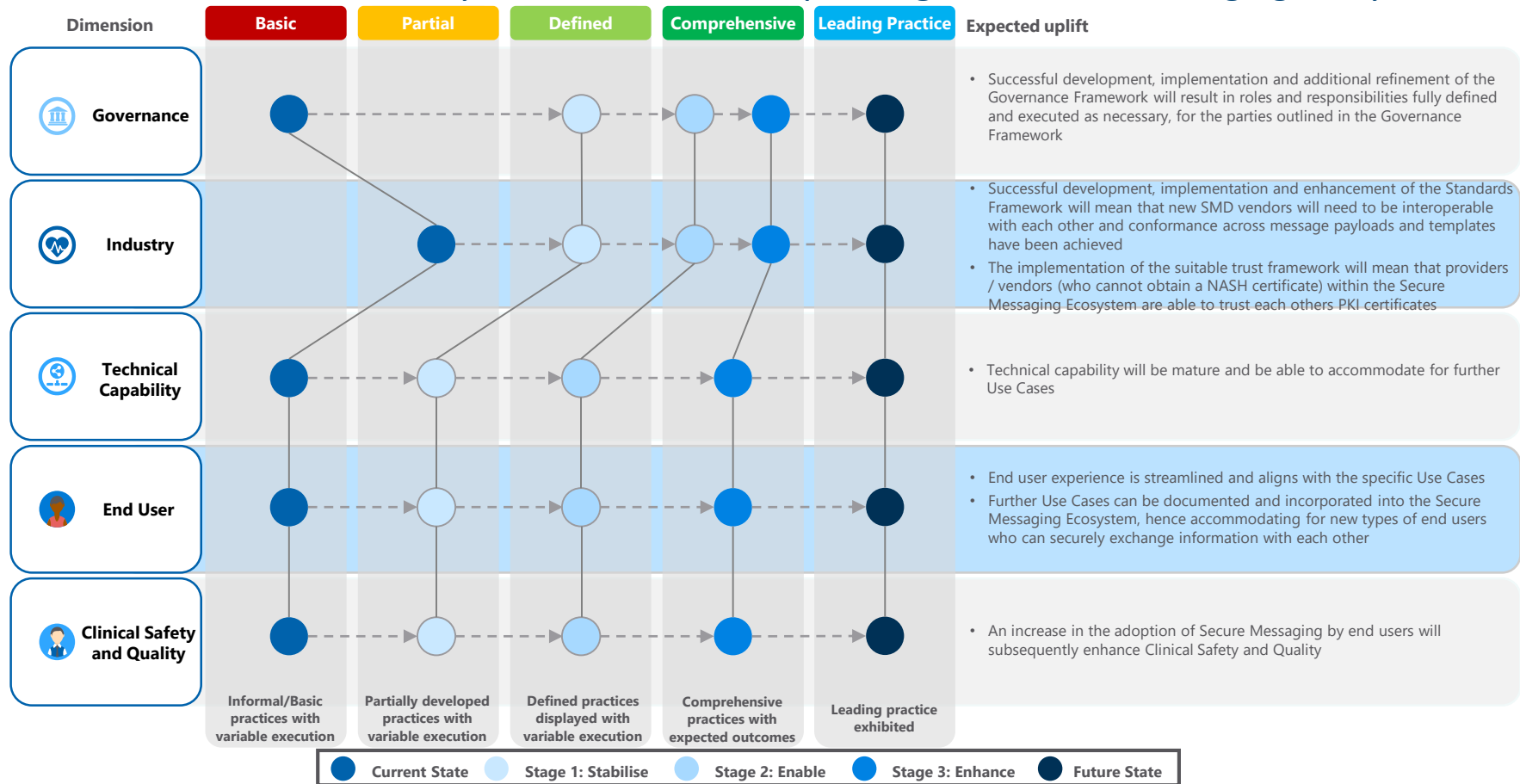
Stage 2: Enable phase will focus on initiatives that aim to achieve conformance, investigate levers that can be incorporated and establishing the change and adoption program



Stage 3: Enhance phase will focus on accelerating planned implementation activities or further enhancement of identified initiatives









In order to demonstrate “Leading Practice” across all dimensions of the framework, further enhancement activities may need to occur for expanding the Secure Messaging Ecosystem



Recommended Next Steps



Recommended next steps for the execution of selected initiatives is detailed below

-  Develop a clear and concise project plan that acknowledges dependencies and timelines of current projects
-  Develop a business case for each initiative
-  Define and agree on clear KPIs for each initiative
-  Develop a high level activation plan that showcases how each department within the Agency is to be involved in each initiative
-  Establish project teams to deliver each initiative
-  Identify the most impactful use cases and / or quick wins



Appendix



An overview of the consultation that was undertaken by Deloitte during the period of the engagement is listed below

Workshop/Session	Stakeholder(s)	Duration	Proposed Date and Time	Project Week	Location
Kick Off Meeting	Neeraj Maharaj, Travis Hodgson	1 x 1.5-2 hour meeting	24 July, 11:30am – 12:30pm	22 July – 26 July	Sydney, Deloitte office
1:1 Executive Stakeholder Interviews	Bettina McMahon, Travis Hodgson, Peter Del Fante, Nathan Pinskiar, Kieron McGuire, Christian Holmes	1 hour interviews	Travis Hodgson (9 Aug, 11am – 12pm) Bettina McMahon (9 Aug, 3pm – 4pm) Peter Del Fante (16 Aug, 3pm – 4pm) Kieron McGuire (20 Aug, 10am – 11am) Nathan Pinskiar (20 Aug, 3:30pm – 4:30pm) Christian Holmes (21 Aug, 10am – 11am)	29 July – 6 Sept	Sydney, ADHA office or Teleconference
1:1 External Interviews	Grahame Grieve, Kate Ebrill (CSIRO), Cerner, Epic, DXC, Intersystem, Oracle, MMex, Genie, NBN Co. / Telstra, Fred IT, Corum, Health Direct, DHHS, NT Health, Qld Health	1 hour interviews with each external stakeholder	Cerner (19 Aug 3pm – 4pm) Grahame Grieve (21 Aug 11:30am – 12:30pm) Kate Ebrill (21 Aug 11:30am - 12:30pm) Genie (21 Aug 2pm – 3pm) DXC (22 Aug 2pm – 3pm) Fred IT (23 Aug 11am – 12pm) Intersystems (28 Aug 2:30pm – 3:30pm) Telstra / Communicare (27 Aug 3pm - 4pm) MMex (29 Aug 1pm – 2pm) Corum (4 Sept 10am – 11am) Health Direct (6 Sept 11am – 12pm) DHHS (9 Sept 11:30am – 12:30pm) NT Health (12 Sept 10:30am – 11:30pm) ACT Health (12 Sept 11:30am – 12:30pm) Qld Health (20 Sept 2-3pm)	29 July – 20 Sept	Sydney, ADHA office or Teleconference
Secure Messaging Current State Workshop (ADHA)	Bettina McMahon, Travis Hodgson, Peter Del Fante, Nathan Pinskiar, Kieron McGuire, Neeraj Maharaj, Christian Holmes, Rupert Lee	1 x 3 hour workshop	8 Aug, 12pm – 3pm	5 July – 9 Aug	Sydney, ADHA office
External Stakeholder Survey	Receivers and senders of health information (GPs/PHNs, public hospitals, private hospitals, specialists, pharmacists, NDIS, Workers Comp, Corrective Services, etc.)	30 minute to complete the questionnaire	Sent out survey on the week of 19 Aug	5 Aug – 27 Sept	Online
Pain Points & Opportunities Workshop (CI System Providers)	Best Practice, Medical Director, Coreplus, Genie, Telstra Health, Global Health	1 x 3 hour workshop	15 Aug, 9am – 12pm	12 Aug – 16 Aug	Melbourne, Deloitte office
Pain Points & Opportunities Workshop (Secure Messaging Suppliers)	Telstra Health, HealthLink, Medical Objects, Global Health	1 x 3 hour workshop	15 Aug, 2pm – 5pm	12 Aug – 16 Aug	Melbourne, Deloitte office
Prioritisation Workshop	Bettina McMahon, Travis Hodgson, Peter Del Fante, Nathan Pinskiar, Kieron McGuire, Neeraj Maharaj, Christian Holmes, Rupert Lee	1 x 3 hour workshop	12 Sept, 1pm – 4pm	9 Sept – 13 Sept	Sydney, ADHA office, Online
Draft Presentation	Bettina McMahon, Travis Hodgson, Peter Del Fante, Nathan Pinskiar, Kieron McGuire, Neeraj Maharaj, Christian Holmes, Rupert Lee	1 x 1-2 hour meeting	23 Sept, 1:30pm – 3:30pm	23 Sept – 27 Sept	Sydney, ADHA office
Final presentation	Bettina McMahon, Travis Hodgson, Peter Del Fante, Nathan Pinskiar, Kieron McGuire, Neeraj Maharaj, Christian Holmes, Rupert Lee	1 x 1-2 hour meeting	8 Oct, 2pm – 4pm	30 Sept – 4 Oct	Sydney, ADHA office

External Survey Design (1/4)

Definition of Secure Messaging

What is Secure Messaging?

Secure Messaging is used for exchanging clinical information between healthcare providers over a Secure Messaging network. This is achieved between a network of connected clinical information systems or practice management systems. Healthcare providers need to frequently exchange patient information with other members of a patient's care team. This can be done through a messaging exchange service that is secure, seamless and efficient. Secure Messaging has some similarities to an encrypted email or digital fax – but it is neither. A Secure Messaging network is offered and managed by one or more Secure Messaging providers.

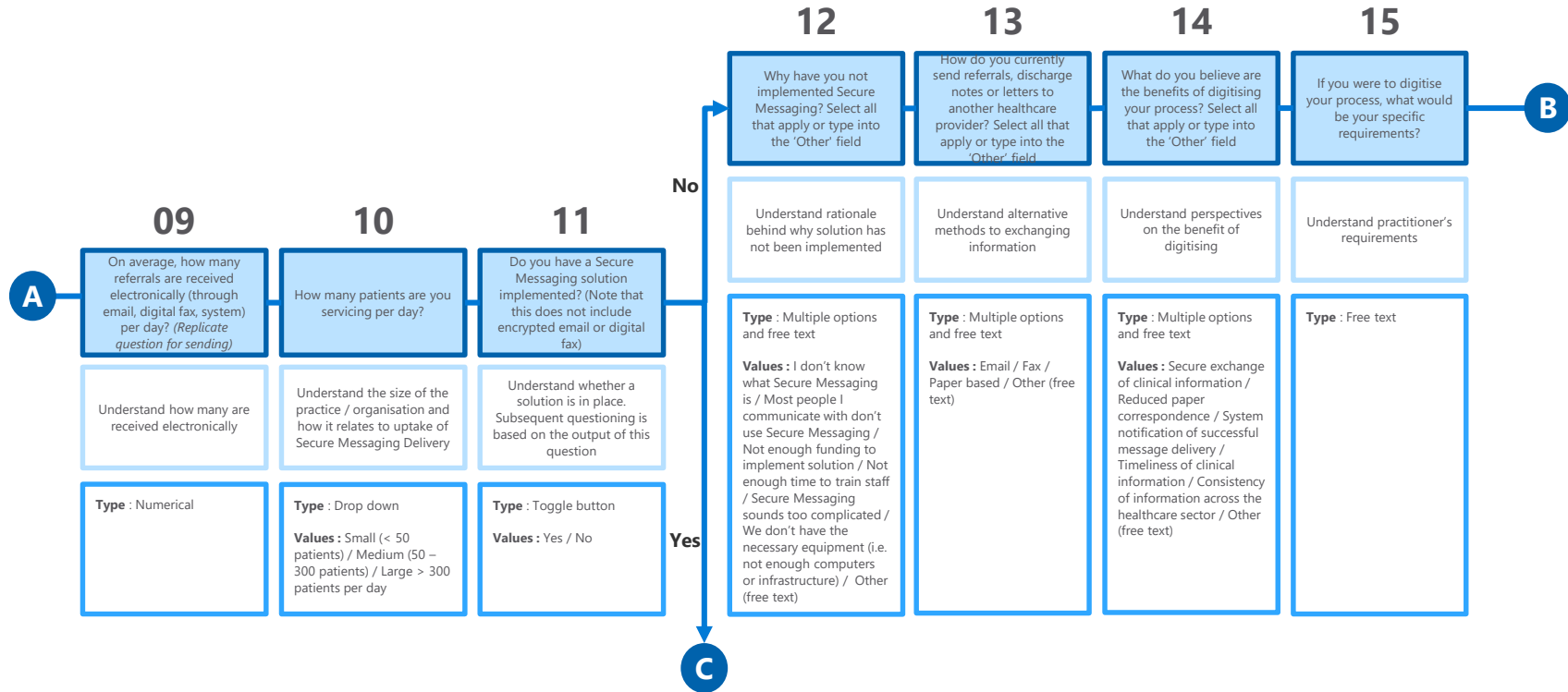
An example scenario is as below:

Doctor Smith needs to send a patient referral to Doctor Williams who works in a different specialist clinic. Doctor Smith accesses his clinical information system, enters the patient referral details and chooses a messaging provider that Doctor Williams also uses. Doctor Smith then sends the referral and the message is securely transferred to Doctor Williams. Doctor Williams accesses his clinical information system and sees that Doctor Smith has sent a Secure Message containing a patient referral. He opens the referral and is able to see the patient referral details.

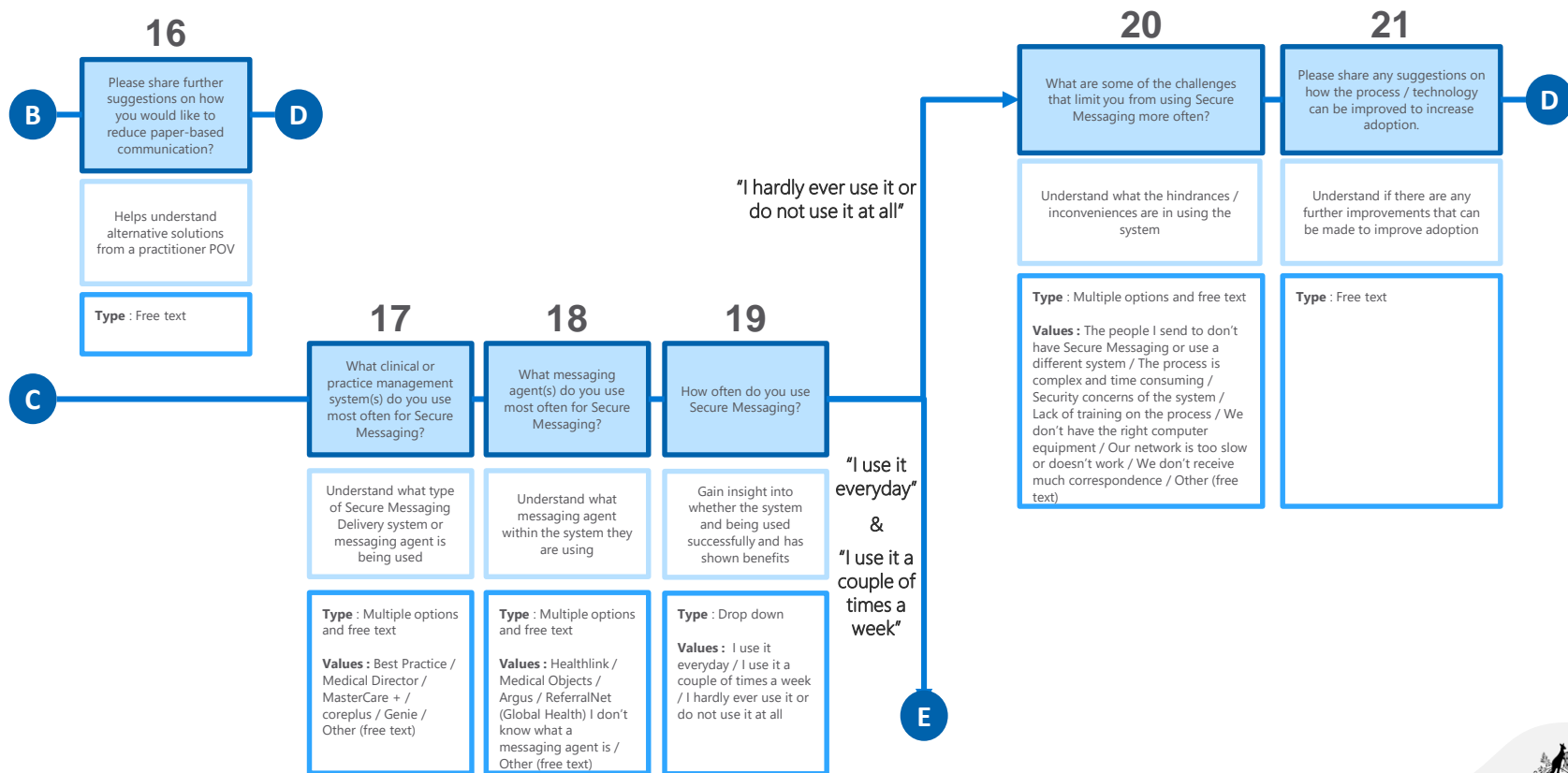
01	02	03	04	05	06	07	08
Where do you work in Australia?	What type of practitioner or healthcare provider are you?	What is your job role?	On average, how many discharge summaries do you receive per day? (Replicate question for sending)	On average, how many discharge summaries are received electronically (through email, digital fax, system) per day? (Replicate question for sending)	On average, how many specialist letters do you receive per day? (Replicate question for sending)	On average, how many specialist letters are received electronically (through email, digital fax, system) per day? (Replicate question for sending)	On average, how many referrals do you receive per day? (Replicate question for sending)
Understand geographical uptake of Secure Messaging Delivery	Understand type of practitioner / institution and how it relates to uptake of Secure Messaging Delivery	Understand the role the end user plays within their organisation	Understand total amount of discharge summaries per day	Understand how many are received electronically	Understand total amount of specialist letters per day	Understand how many are received electronically	Understand total amount of referrals per day
Type : Drop down Values : NSW / QLD / SA / Tas / Vic / WA / NT / ACT	Type : Drop down / free text Values : GP / PHN / Public Hospital / Allied Health Service / Private Hospital / Specialist / Pharmacist / Community Health service / Workers Compensation / Corrective Services / Ambulance Services / Pathology / Radiology / Aged care / Other (Free text)	Type : Free text	Type : Numerical	Type : Numerical	Type : Numerical	Type : Numerical	Type : Numerical

A

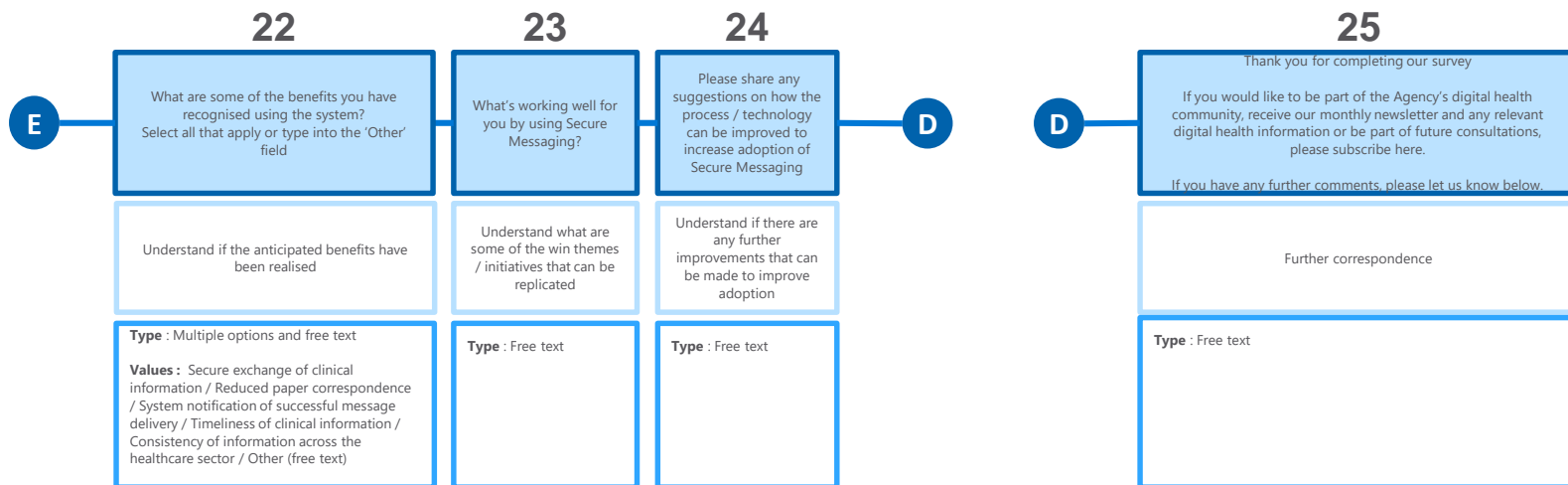
External Survey Design (2/4)



External Survey Design (3/4)



External Survey Design (4/4)



Contact us

Help Centre	1300 901 001
Email	help@digitalhealth.gov.au
Website	digitalhealth.gov.au
Twitter	twitter.com/AuDigitalHealth

