Australian Government
Australian Digital Health Agency

2022-2025 CYBER SECURITY STRATEGY

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

Acknowledgements

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

Disclaimer

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

Document control

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

Chief Information Security Officer (CISO)

TABLE OF CONTENTS

This page has been left intentionally blank.

For external publication

CEO FORWARD

I am pleased to present the Australian Digital Health Agency's *Cyber Security Strategy 2022 – 25*.

The Strategy sets the vision and guiding principles for our cyber security over the next three years. It sets out our approach to and areas for action on cyber security, but will also be regularly reviewed to ensure we proactively adapt to changes in the threat environment and support the secure evolution of digital health.

The Australian Government recognises the importance of cyber security to Australia's growing digital economy and to the Australian community. Through this Strategy, the Australian Digital Health Agency will build on our strong foundations and elevate our organisational capability to securely deliver better health and wellbeing for all Australians, supported by safe, secure digital systems.

As Australia's champion for digital healthcare, we are responsible for the development, deployment, and secure operation of critical national healthcare assets, including the personal and sensitive healthcare information of Australians. We take this responsibility seriously.

We are also part of many interconnected IT systems across the health sector and are charged with helping ensure information can be shared quickly and easily across those systems to support best practice healthcare.

In doing so we recognise that our work is dynamic, as are the digital and threat environments we work in. The pandemic has reinforced this, underscoring the need to achieve and maintain the future focused cyber capabilities that will enable us to be proactive in how we protect ourselves, each other and the health information of Australians.

This Cyber Security Strategy sets out our coordinated, holistic approach to uplifting capability across the Agency in response to this changing cyber environment. It also provides a clear plan to meaningfully support Australian healthcare providers and health technology partners to protect themselves and the critical health information they too hold.

Cyber security is not a technical niche. Everyone at the Agency and in the healthcare community has a part to play. Our success will be underpinned by our security culture, secure business practices and by our behaviours - at home and at work. It will be defined by our dedication to change and willingness to embrace the challenges ahead. The spirit of innovation and passion to improve the health and wellbeing of Australians animates the Australian Digital Health Agency. Our cyber security must also embody this spirit so that together we can set a new standard for secure innovation, continuous improvement and digital health reform in Australia.

Amanda Cattermole, PSM

CEO

EXECUTIVE SUMMARY

The Role of the Agency

The Australian Digital Health Agency is responsible for Australia's critical digital health infrastructure and plays an important role in the provision of core services to meet the needs of the healthcare industry and the broader Australian public. To operate effectively, the cyber security of these critical national assets and the Agency itself must be assured.

The Agency operates at the heart of Australia's digital health ecosystem, bringing together public infrastructure and industry innovation to meet the health and wellbeing needs of all Australians. This important work has already transformed the quality, accessibility, and sustainability of health and care in Australia, and it will continue to do so at an increasingly rapid pace. The COVID-19 pandemic has prompted a seismic shift in the take up of digital health services across Australia. By every metric, engagement with digital health has increased. Across Australia's health ecosystem, healthcare providers, health technology partners and consumers have all come to trust in and rely on digital platforms to store and access health information. This has necessitated a rapid expansion in the Agency's platforms and the services they support.

In the future, the Agency must accommodate a large, expected increase in the volume of health information. It will be critical that services and supporting infrastructure and platforms remain fit for purpose and cyber resilient, even as changes occur in the cyber threat environment, where both the pace of change and the level of risk are elevated. The Agency understands that the consequence of compromise to any asset within its digital healthcare ecosystem would be serious. Digital health information is sensitive, personal and its confidentiality must be maintained. Accordingly, the Agency will continue to build on its cyber security successes to date by working to address the highest risk elements of the cyber threat environment, while supporting the Australian healthcare community to do the same. Cyber security at the Australian Digital Health Agency will continue to play a critical dual role in providing proactive protection to Agency assets while supporting uplift across the Australian digital healthcare ecosystem.

The Strategic Direction for Cyber Security

The Australian Digital Health Agency has set itself the vision of becoming a leading cyber capability that can enable the next frontier of digital health and support the resilience of the Australian healthcare ecosystem. As the Agency shifts focus from custodianship of My Health Record to championing digital health in Australia, the Agency's cyber security workforce, capabilities and functional alignments will change to support this new evolution in responsibility and remit.

This intent and the key strategic elements of this strategic direction are presented on pages 10-11.

Guiding Principles

In support of this ambition, four guiding principles will be applied to shape how the Agency will work, think, and behave:

- *Business-Led.* Cyber security services and solutions are aligned to strategic Agency objectives and clinical outcomes.
- *Future Focused.* Staying ahead of the evolving digital healthcare environment, ready to securely support the next horizon of digital health.
- *Prioritised Effort.* Resources are focused on maximising value for the Agency and the Australian healthcare ecosystem.
- *Security By Design.* Creating a DevSecOps environment that fully integrates security into every stage of product development.

Focus Areas

Over the next three years, these principles will be applied across a programme of work, spanning four interconnected focus areas that represent the building blocks of the Agency's future cyber system:

- *Governance & Operations.* The Agency will optimise its governance and operations, enabling improved decision-making, strategic planning, and prioritisation.
- *Security Culture.* The Agency will strengthen its security culture and uplift cyber awareness by enhancing and role-modelling cyber security behaviours, at work and at home.
- *Workforce Investment.* The Agency will continue to invest in its people and Australia's cyber future by strengthening upskilling and cross-skilling programs and introducing new pathways for direct entry.
- *Capability & Proportionality.* The Agency will take a risk-optimised approach to capability development, building our agility and ability to preemptively focus on new technical innovation and areas of highest risk.

The Agency is both responsible for securing Australia's personal and sensitive health data and ensuring that health information is accessible to providers and consumers throughout the digital health ecosystem, supporting digital innovation. The Australian Digital Health Agency's cyber security must continue to maintain a balance across this dual focus. Over the next three years, the cyber security of the Australian Digital Health Agency will be supported to achieve this balance through investment across the Agency's cyber security workforce, capabilities, and functions, as described by this Cyber Security Strategy.

This page has been left intentionally blank.

STRATEGIC DIRECTION

OUR CYBER FUTURE

To meet this complex operating environment, it is vital that the Australian Digital Health Agency retains an advanced cyber security capability that can evolve to stay ahead of advances in digital health technology and the dynamic cyber environment.

Accordingly, the Agency's Strategic Vision for cyber security over the next three years is:

CYBER SECURITY THAT ENABLES THE NEXT FRONTIER OF DIGITAL HEALTH BY SUPPORTING A RESILIENT HEALTHCARE ECOSYSTEM

The Strategic Vision is supported by four guiding principles that will shape how the Agency will work, think and behave to achieve the Vision:

BUSINESS LED

Cyber security services and solutions are aligned to strategic Agency objectives and clinical outcomes.

FUTURE FOCUSED

Staying ahead of the evolving digital healthcare environment, ready to securely support the next horizon of digital health.

PRIORITISED EFFORT

Resources are focused on maximising value for the Agency and the Australian healthcare ecosystem.

SECURITY BY DESIGN

Creating a DevSecOps environment that fully integrates security into every stage of product development.

To achieve the Strategic Vision, the Agency will undertake a three-year programme of work across four focus areas in alignment with the four guiding principles. These focus areas represent the building blocks needed to establish the Agency's future cyber security system:

CAPABILITY & PROPORTIONALITY

The Agency will take a risk-optimised approach to capability development, building our agility and ability to preemptively focus on new technical innovation and areas of highest risk.

WORKFORCE INVESTMENT

The Agency will continue to invest in its people and Australia's cyber future by strengthening upskilling and cross-skilling programs and introducing new pathways for direct entry.

SECURITY CULTURE

The Agency will strengthen its security culture and uplift cyber awareness by enhancing and role-modelling cyber security behaviours, at work and at home.

GOVERNANCE & OPERATIONS

The Agency will optimise its governance and operations, enabling improved decision-making, strategic planning, and prioritisation.

Building on the Agency's strong security foundations, this prioritised programme of action will ensure that the Agency is able to stay ahead of changes in the cyber environment and is positioned to support and secure the future digital health for all Australians.

STRATEGIC CONTEXT

STRATEGIC CONTEXT

The Agency's Operating Context

The Australian Digital Health Agency is at the forefront of Australia's digital health operating environment. This means that the Agency is expected to provide critical infrastructure services and facilitate the operation of a wide portfolio of digital health services that meet the needs and high standards of individuals, healthcare providers, service providers and the broader Australian community. The COVID-19 pandemic has created a seismic shift in the uptake of digital health services, including Telehealth and electronic prescription services, in Australia. This has created a growing need to accommodate increases in the volume of health information exchange, further improvements to services, and the changes required to ensure supporting infrastructure and platforms are well managed and fit-for-purpose. At the same time, the Agency must continue to focus on the protections associated with ensuring the confidentiality of Australian personal health information.

The Australian Digital Health Agency's scope of work is now shifting from laying Australia's digital health foundations, including the My Health Record system, to taking on the role of Australia's champion of digital health. This evolution in scope entails an increase in responsibility. Accordingly, the Agency's cyber security workforce, capabilities and functional alignments must accommodate and enable the new direction.

The Cyber Environment

The cyber environment the Australian Digital Health Agency and the broader Australian healthcare sector operate in is complex, evolving, and high risk. As with other areas of the Australian economy, COVID-19 has acted as a catalyst for change in healthcare. Healthcare providers and individuals have come to trust and accept digital health services, leading to an exponential increase in the uptake of Agency services. Simultaneously, the cyber environment has also become increasingly congested and contested. The Agency must adapt to these changes whilst continuing to ensure the security of personal sensitive health information, even as cyber risk levels also continue to increase.

The Agency recognises that the consequences of compromise to any asset forming part of the Agency digital healthcare ecosystem would be serious. The digital connections that link the Australian healthcare ecosystem together are powerful but may be exploited if not managed securely. Not only must the Australian Digital Health Agency continue to manage high levels of cyber risk, it must also be prepared to support the Australian healthcare community to do the same. The Agency's cyber security function must continue to evolve, providing proactive protection to Agency assets and supporting uplift across the Australian digital healthcare ecosystem.

Regulatory and Legislative Changes

The Australian regulatory landscape is also continuing to evolve in response to trends in the cyber threat environment. Changes to legislation will further shape the role the Agency plays in securing Australia's digital health ecosystem.

- The Agency continues to monitor and support the ongoing review of the **Privacy Act 1988 (Cth).** This includes the introduction of the **Online Privacy Bill** to encourage harmonisation and interoperability of privacy and security obligations between **My Health Records Act 2012 (Cth)** and the **Privacy Act 1988 (Cth).** This will ensure that all digital innovation is equipped with strong security, privacy, and clinical safeguards.

- The strengthened security and privacy protections introduced by the **Trusted Digital Identity Bill** will enable secure and streamlined access to both public and private sector services forming part of the digital health ecosystem.
- The Agency has prioritised recommendations outlined in the **My Health Records Act Review**, including increased monitoring of healthcare and service providers' compliance with legislative requirements to effectively manage shared cyber security risks.
- The Agency will support the recent and anticipated amendments to the **Security of Critical Infrastructure Act 2018 (Cth)** and the **Ransomware Payments Bill 2021 (Cth)** with a program of awareness and education initiatives to ensure that critical infrastructure assets and critical infrastructure sector assets within the digital healthcare ecosystem are aware of their cyber reporting and management obligations and receive the appropriate level of cyber security support from the Agency. As an organisation operating in a critical infrastructure sector, the Agency is equally focused on a strong internal and external cyber security risk management.
- The Australian Government is seeking to strengthen and coordinate the management and operation of its IT networks through the establishment of **Cyber Hubs**. This centralisation aims to consolidate cyber security services across Australian Government Agencies.

Alignment to the National Digital Health Strategy

The Agency's Cyber Security Strategy is closely aligned with the National Digital Health Strategy, demonstrating a unified vision for the future, and security, of digital health. This is illustrative of the close, enabling relationship that must always exist between cyber security and the digital health services provided by the Agency.

It is only by working together that the Australian Digital Health Agency and the Australian healthcare community will be able to continue strengthening our individual and collective cyber posture, and achieve the Strategic Vision presented in this, the Agency's Cyber Security Strategy.

FOCUS AREAS

1 STRUCTURE & GOVERNANCE

The Australian Digital Health Agency’s role is evolving to more fully encompass the designing, building, and running of digital health platforms on behalf of Australia. This, alongside the demand for digital health prompted by the COVID-19 pandemic, has necessitated a rapid expansion in Agency platforms and services. The digital healthcare ecosystem will continue to expand into a multi-partner, multi-product, omni-channel environment, and continuing to securely manage this growing complexity is a key strategic priority. Accordingly, internal Agency cyber security governance and operations must pivot to support, protect, and enable this expansion.

Uplifting and strengthening cyber security governance for the Australian Digital Health Agency will not be a single activity. Rather, it will be a systematic approach to designing and implementing the organisational elements and structures needed to position the Agency to respond to and strategically manage change. Already, shifts in the cyber, legislative and digital environments are affecting the way services must be delivered. In the future, these changes and the pace at which they occur can only be expected to accelerate, requiring the Agency to also manage periods of heightened uncertainty, increased pace and elevated risk.

The Agency will ensure that internal cyber security structures and governance arrangements can effectively manage and support this growing volume of complex digital assets in the high risk, and changeable, cyber threat environment it must operate in. By optimising how cyber security functions are arranged and embedded into the workings of the Agency, the Australian Digital Health Agency will uplift how cyber security is governed and incorporated into corporate operations, enabling enhanced decision-making.

As such, this focus area is designed to support high performance, accountability and control across the Agency. It will build on the Agency’s strong foundations to strengthen how risk and performance is managed to enable and secure a complex and evolving digital healthcare ecosystem. It will also enhance the processes that ensure the Agency is able to meet its security obligations, including evolving legislative requirements, to Government and the Australian people. Streamlining internal workflows will establish an Agency-wide understanding of cyber requirements, touchpoints and the roles and responsibilities of cyber teams. This will support and accelerate the planned transition to more agile delivery methods, such as DevSecOps, by efficiently embedding cyber security by design into every phase of the Agency’s delivery processes. In turn, this will foster a culture of agile coordination and collaboration whilst also enhancing opportunities for secure partnerships across the Agency and the broader healthcare ecosystem.

STRATEGIC OBJECTIVES

This focus area will deliver:

- Enhanced decision-making, improving Agency capacity to preempt and rapidly react to changes in the security environment in a coordinated manner.
- Strengthened cyber security engagement processes, fully integrating security by design into Agency delivery methodologies.
- Strengthened visibility of risk and Agency performance, supporting a high-performance security culture, and enabling the realisation of efficiencies across the Agency’s digital delivery lifecycle.
- Enhanced internal collaboration, promoting increased cyber awareness across the Agency, government partners, healthcare providers and the broader community.

2 SECURITY CULTURE

The Australian Digital Health Agency operates in an expanding digital healthcare ecosystem. Healthcare providers, service and technology providers and the broader Australian community trust in and rely on digital platforms to store and access sensitive and confidential health information. As such, security must continue to be embraced as an important and constructive capability by the Agency as well as the broader digital healthcare sector. It must be embedded into how people think and behave.

The Agency is committed to establishing a positive Agency-wide security culture, underpinned by shared values, attitudes and behaviours. A united security culture will ensure that security values and behaviours will be consistently reflected in the actions of Agency personnel, healthcare providers, service providers and the broader Australian public.

The Agency must continue to promote good cyber security practices and uplift cyber awareness to establish an Agency-wide understanding of cyber security, its importance and the roles and evolving responsibilities of cyber teams. Over the next three years, the Agency will continue to uplift cyber awareness across the digital health ecosystem by facilitating a top-down approach to cyber security through the implementation of cyber security culture initiatives. This will see greater engagement with cyber security processes and a growing recognition that effective security is critical to the Agency's operation.

Simultaneously, the Agency will promote updates to its cyber security operating model to uplift internal awareness of cyber processes and support enhanced cyber governance. Continuous communication will also be key to establishing an effective security culture as it will ensure that security is actively lived throughout the Agency. The establishment of this proactive, positive security culture, underpinned by advanced cyber awareness, will ensure that good cyber security practices and behaviours can be role modelled across the Agency.

An effective security culture must be embraced by everyone at the Agency. This requires greater engagement with cyber security and acceptance of personal responsibility for security issues. By establishing an understanding that security is everyone's responsibility, the Agency will be better placed to meet the increased demands of healthcare providers and consumers to protect and secure Australia's digital health information.

STRATEGIC OBJECTIVES

This focus area will deliver:

- Enhanced understanding of the Agency's cyber security operating model and governance structures to encourage the visibility of good cyber security practices.
- A top-down approach to cyber security culture, supporting stronger Agency-wide understanding of cyber security and its significance.
- Leading cyber security behaviours instilled in Agency personnel, healthcare providers and consumers within the digital health ecosystem to ensure the protection and confidentiality of digital health information.
- An enhanced security culture underpinned by shared values and behaviours to ensure that security is understood as an individual responsibility.

3 WORKFORCE INVESTMENT

Internal Agency cyber capabilities will continue to expand to support and enable the rapidly evolving future of digital healthcare. This must be underpinned by a mature cyber workforce. Within the context of the national skills shortage, attracting and retaining cyber and technical talent continues to be challenging for all organisations. Recently, the COVID-19 pandemic has also created new challenges. It has fundamentally reshaped ways of working and traditional means of access to national and international talent markets, putting further pressure on Australia's already depleted skills pool. It is only by holistically investing in the Agency workforce, across all functions and levels, that the Agency will be able to continue to grow its cyber talent and protect the future of digital health for all Australians.

The amount of personal, sensitive health information, and the ways it can be used to support better health for all Australians, continues to multiply. Simultaneously, the Agency's obligation to ensure the cyber security of this information and new, novel ways of using it, will grow. Doing this has a critical dependency on maturing and expanding the cyber skillsets of the Agency's existing workforce, whilst also creating more pathways for Australians from all walks of life to embark on a cyber career.

Over the next three years, the Agency will invest in strategically planning its future cyber workforce needs, maintaining a dual focus on attracting new talent, and retaining the skills and Agency-specific knowledge that has been nurtured in current cyber teams. Investing in the cyber security professionals currently working at the Agency will ensure skills are contemporary and ready for the next frontier of digital innovation, providing exciting and fulfilling cyber careers. Simultaneously, lateral cross-skilling opportunities and entry-level cyber pathways will be created to build the capacity that will be needed to support the advanced, proactive protection capabilities of the future.

COVID-19 has created new opportunities for remote working and better integration of flexible, agile work practices. The Agency has been successful at adapting to this new normal. Building on these successes, the Agency will continue to enhance its value proposition for cyber security and technical professionals while also enhancing the value the Agency provides to the healthcare ecosystem through opportunities to uplift healthcare-focused cyber.

STRATEGIC OBJECTIVES

This focus area will deliver:

- Enhanced strategic workforce planning that optimises management of Agency cyber employee lifecycles and professional pathways.
- A strengthened employee value proposition that establishes the Australian Digital Health Agency as a technical and cyber employer of choice.
- Enhanced cyber expertise that is always contemporary and able to proactively protect the Agency, and support Australia's digital healthcare providers and systems.
- A larger national cyber talent pool where diversity is encouraged and support is tailored to allow underrepresented cohorts to take up new cyber opportunities.
- Strengthened connections and support systems between those at the nexus of cyber and health across the digital healthcare ecosystem.

4 CAPABILITY & PROPORTIONALITY

By aligning cyber capabilities and investments with strategic business objectives, the enterprise risk profile and the cyber threat environment, the Australian Digital Health Agency will pursue an efficient, targeted approach to cyber investment that optimises effort to effectively protect Australia's digital healthcare ecosystem.

As the amount of sensitive, private health information within the multi-product, multi-partner, omnichannel digital environment continues to increase, the Agency must ensure capable and proportionate cyber security to support Australia's expanded digital health landscape. This necessitates continuing to address capability gaps and enterprise risk factors with targeted investment in the Agency's cyber portfolio.

As Australia's digital healthcare champion, the Agency will ensure its suite of cyber capabilities reflects critical business objectives, planned digital services, and intelligence about the cyber threat environment. This will commence with establishing a risk-optimised, intelligence-led approach to capability investment that focuses on targeted uplift across current tooling and aligning future investments to enterprise risk reduction activities.

Capability development will be pursued alongside a strengthened centralised planning function to enable the Agency to fully realise the benefits of this approach, as well as achieve efficiencies across related workflows. Initial uplift priorities will encompass incident response, recovery and threat intelligence capabilities, as these are directly tied to current areas of risk and high priority workflow improvements. Further investments will build on this program of work to create a robust and resilient cyber security system, capable of protecting the future of Australia's digital healthcare.

Following this approach, capability investments will not be limited to the procurement of tools. Capability will be considered in its entirety. Accordingly, strategic plans will encompass elements such as the number of people, skill types and workflow processes needed to operate a cyber security system at a level commensurate with the cyber threat. This will also include the sustainment, retirement and replacement requirements that must be considered as part of the overall lifecycle to ensure the Agency's cyber portfolio is equipped to protect future digital healthcare innovation, as well as the core health services and platforms that are critical to the health and wellbeing of Australia.

STRATEGIC OBJECTIVES

This focus area will deliver:

- An integrated portfolio of cyber security capabilities that works as a system of systems to reduce enterprise risk and address likely cyber threats.
- An enhanced strategic planning function that enables the Agency to fully realise the benefits of investments across all elements within the capability lifecycle.
- Improved alignment of cyber capabilities with the threat environment to support proactive protection of Australia's expanding digital health landscape.
- Heightened efficiency in the delivery of cyber security services to Agency projects, critical national health infrastructure, healthcare providers and consumers throughout the Australian healthcare ecosystem.

NEXT STEPS

NEXT STEPS

The Australian Digital Health Agency is committed to achieving the evolution of a safe, secure, and seamless digital health capability, to the benefit of all Australians. While ambitious, the Strategic Vision described in this Strategy outlines a cyber secure future that must be realised to support this commitment. Security underpins the Agency's strategic priorities and achievements in digital healthcare to date. It will remain a critical enabler into the future.

Through this Cyber Security Strategy, the Australian Digital Health Agency will embark on a programme of strategic cyber security uplift. Over the next three years, the Agency will work to optimise operations and governance arrangements, strengthen security culture, invest in both the current and future cyber workforce, and build agility and proactive protection into future cyber security capabilities.

In doing so, the Agency will achieve the future focused cyber security posture required to support cutting edge digital healthcare innovation, while ensuring the security of Australian digital health services and sensitive personal health information.

.

Australian Government
Australian Digital Health Agency

CyberCX

digitalhealth.gov.au