imprivata®

WHITEPAPER

Connected, secure, efficient: Transforming aged care through better access to patient information

Ageing Australia®

Imprivata is proud to be an affiliate of Ageing Australia

Imprivata | Ageing Australia

01

Executive summary

As the aged care industry evolves to meet the current and future needs of Australia's citizens, technology is set to play a key role.

Digital transformation across the sector will enable organisations providing aged care services to meet new government requirements for the quality of care provided. Requirements include a minimum number of minutes of care per resident per day, some of which should be provided by a registered nurse, and all of which must be accurately documented in order to secure Government funding.

The Government's Aged Care Worker Survey 2024 report finds that most people work in aged care because they want to make a difference to older people's lives. Yet many of them work extra unpaid hours because there is more work to do than they can get through during their shifts.

There is also now a greater emphasis placed on the experience of the people receiving the care. When workers are stressed because they cannot access resident information quickly, have forgotten a complex password, or are writing notes by hand to manually input to the system after their shift ends, their attention is diverted, to the detriment of the resident.

Technology will provide a platform for increased efficiency and greater user engagement, freeing up nurses and care workers to focus on care participants and do what they signed up for – looking after people.

This whitepaper sets out the challenges and then explains how connected, secure, and efficient access to resident and clinical information pays dividends. Imprivata Enterprise Access Management saves time for busy clinicians, nurses, and care workers, improves cybersecurity, protects resident confidentiality, and supports improved compliance. Read on to find out more.

"Feedback has been amazing from our carers and clinicians working across all Sundale facilities that have adopted the new solution. Everyone loves Imprivata tap on/ tap off."

– Grant Morris, ICT Project Manager at Sundale Ltd.

02

Introduction: The state of Australian aged care

The Treasury of the Australian Government's Intergenerational Report forecasts that by 2062, the number of people aged over 65 is expected to more than double. The number of people over the age of 85 will more than triple. The aged care sector workforce, which is already under strain, will need to increase to meet this demand.

As well as meeting the pressure of increasing demand, the sector is also tasked with improving the quality of care provided. On 1 November 2025, the new Aged Care Act 2024 commenced, bringing key changes to how aged care providers operate and the obligations they must meet. Two of the guiding principles are:

- **Trusted –** Trust, privacy, and security need to be safeguarded. Consent, confidence, and trust in how personal information is used and protected are fundamental. Initiatives involving sensitive information sharing are tightly controlled to protect individuals' privacy.
- **Care-focused –** Burden for frontline workers should be minimised so they can focus on providing high-quality care. Implementation of actions ensures the important work of aged care workers is supported by tools and processes that allow them to focus on providing quality care to older people.

In order to qualify for funding under the Australian National Aged Care Classification (AN-ACC) model, organisations must provide mandatory minutes of care per resident, per day. In addition, there is now a greater focus on the experience of the people receiving care.

The sector is transitioning, although, according to the Inspector-General of Aged Care – 2025 Progress Report on Royal Commission Recommendations, progress has not been as swift as originally hoped. The StewartBrown Aged Care Financial Performance Survey Report notes that the sector, in general, is not making enough margin on services provided. If the aged care sector is to rise to meet the challenges it faces, better use of technology and digitisation will help to deliver care more effectively, more efficiently, more safely, and more profitably.

According to the Australian Hospitals and Healthcare Association's digital maturity models for primary healthcare, digital information, when used appropriately, has the potential to transform the quality and sustainability of health and healthcare services. Digital technologies are increasingly seen as essential resources in primary care, with common uses including clinical decision support systems, quality of care, tracking of medical supplies, and infectious disease surveillance. While Aged Care is not strictly speaking primary care, it is closely aligned and uses many of the same systems, including the electronic medical/care record (EMR/ECR).

Advancing data and digital technologies will also help aged care providers to:

- Manage current and future service demand
- Reduce administrative burden
- Give workers more time to spend on direct care

This point is underlined by the Government's Intergenerational Report, which suggests that up to one-third of time spent on administrative tasks can be saved by implementing digital technology, increasing the digital capability of the aged care workforce, and introducing new policies on data sharing. Based on departmental work projections, digital enablement also has the potential to reduce the predicted shortfall in the aged care workforce.

By eliminating laborious administrative tasks, such as long, complex logins entered multiple times per hour, residential care facilities create a more fulfilling work environment where staff can focus on providing care. This, in turn, helps facilities to attract and retain key workers. With strong access management in place, carers have fast, secure access to resident information, enabling them to do what they're best at – caring for residents.

03

Regulatory drivers shaping identity and access governance

While the increased adoption of digital technology will help the aged care sector become more efficient and provide a means to prove that appropriate care is being provided, there may still be barriers to adoption among less tech-savvy staff. An increase in digital tools also brings increased risks to patient privacy and opens the door to cyberattacks.

Furthermore, alongside changes to the care landscape, digitisation also introduces additional regulatory requirements. For example, the Privacy Act Amendment 2024 has increased penalties for privacy breaches and strengthened breach notification requirements.

"Imprivata has enabled us to greatly increase data security AND improve the user experience. These two goals are no longer mutually exclusive as has been the case in the past, thanks to Imprivata."

– Lani Maxfield, Senior Systems Engineer, Sundale Ltd.

As one of Australia's 11 designated critical infrastructure sectors, healthcare and medical is subject to the 2023-2030 Australian Cyber Security Strategy and must be able to withstand and bounce back from cyberattacks. The Strategy sets out a bold vision for Australia to be a world leader in cybersecurity by 2030. Key to this goal is protecting the critical infrastructure on which Australia's essential services rely.

Beyond the personal toll on victims, identity theft has a substantial collective impact on society at large. The most recent survey, in 2019, indicated that identity theft has cost Australia more than $3.1 billion and affected 20% of Australians. If identities can be easily stolen or defrauded, communities may lose trust in public institutions, including aged care residential facilities.

The use of technology, such as single sign-on (SSO), provides authorised users with fast, secure access to clinical systems, while also creating an audit trail of who provided what care or treatment to whom and when. This ensures compliance with information governance regulations. In addition, when users no longer need to remember complex passwords, a significant burden is removed from the IT helpdesk. Industry sources estimate that password-related calls to the IT helpdesk can account for 40-50% of tickets. Reducing call volume frees up IT staff to focus on more proactive and fulfilling work.

04

The digital transformation imperative

Modern aged care requires a growing number of digital applications to deliver connected, efficient, and safe services. This includes resident care software (electronic care records, or ECR), clinical applications accessed at the point of care via mobile devices, and an increasing number of connected devices, i.e., the Internet of Medical Things (IoMT). All these systems need to be easy to access and to use, and must be consistently maintained and updated by IT. As the reliance on and complexity of these systems grow, so does the burden on IT teams to ensure that applications remain up to date and as protected as possible from malicious actors looking to disrupt systems and steal lucrative patient information.

The proliferation of digital systems means that healthcare workers now need to perform multiple logins to access information in different systems. These login credentials often include long, complex passwords to safeguard patient information, making them time-consuming and inconvenient to enter while wearing gloves or using mobile devices with small or no keyboards.

Not only are care workers required to log in to access patient information many times during a shift, but carers also need to authenticate when witnessing or prescribing medicines, which further adds to the IT burden and potentially contributes to staff burnout.

Growing reliance on digital systems also increases the potential for a debilitating cyberattack. To help organisations protect against the disruption caused by a serious outage of systems, the Australian Signals Directorate (ASD) has developed prioritised strategies to mitigate cybersecurity incidents.

The most effective mitigation strategies are the Essential Eight, listed here:

- Patch applications
- Patch operating systems
- Implement multifactor authentication (MFA)
- Restrict administrative privileges
- Control applications
- Restrict Microsoft Office macros
- Harden user applications
- Perform regular backups

These mitigation strategies are significantly supported and enabled by implementing technologies such as Imprivata Enterprise Access Management with SSO and MFA, Imprivata Mobile Access Management, Imprivata Mobile Device Access, and Imprivata Privileged Access Security.

05

Core aged care challenges and how Imprivata addresses them

Aged care organisations manage a complex balancing act: keeping care workers efficient and effective, with fast access to digital systems – while also keeping those systems secure. In short, IT must let the good guys in while keeping the bad guys out. Accomplishing this presents IT teams with a series of challenges.

Challenge 1: Workforce mobility

The Australian government is committed to raising the quality of aged care by building a skilled, valued, and supported workforce. Strengthening the aged care workforce is essential to providing older people with the high-quality care they deserve. According to the Aged Care Worker Survey 2024 report, most respondents choose to work in aged care to make a positive change in the lives of older people. However, many are doing unpaid work on top of their contracted hours, often because there is simply too much work to do.

The requirement to log into many different systems multiple times per shift is time-consuming and distracts clinicians from their patients. Imprivata Enterprise Access Management with SSO and badge-tap authentication gives care workers near-instant access without the need to remember complex passwords. This frees up carers to focus on delivering the appropriate care and improving the experience of residents.

MFA, which can use biometrics and FIDO badges, is fast and secure, even when care workers are wearing PPE or gloves. And as carers move from location to location throughout their shift, a simple tap-on/tap-off to access resident information lets them quickly and easily access all the applications they need.

Challenge 2: Clinical efficiency

Fast, frictionless access to clinical information saves significant amounts of time. A peer-reviewed study conducted between 2018 and 2024 across **55 urban hospitals** in the UK and Ireland examined the time savings associated with SSO and demonstrated considerable benefits. Clinicians experience a **60% reduction in desktop login time** and over **50% faster application access** with SSO. Specifically, the research showed that **3.3 million clinician hours** were redirected annually from logging into patient care – equivalent to over **278,000 clinician shifts** of 12 hours duration across the 55 participating hospitals.

While SSO is not focused on cost-cutting, the reclaimed time can help improve patient throughput, staff satisfaction, resource use, and patient care. On average, each hospital gained nearly **AUS$2.02 million/year** in the value of freed clinician time, demonstrating a substantial return on investment.

Imprivata Mobile Access Management (MAM) provides additional benefits by streamlining mobile device use. MAM allows clinicians to select a device from the docking station that has been reset from previous sessions, and is now charged and ready to go.

Challenge 3: Cybersecurity threats

Healthcare organisations are among the top targets for cybercriminals seeking to profit by stealing ultra-sensitive, highly valuable patient information. To protect this data, IT teams face the challenge of granting care workers the access they need to treat residents, while also ensuring that cybersecurity processes meet stringent data protection regulations. Passwords are often the weakest link in the security chain because they can be hacked, phished, or guessed. The use of generic accounts or shared credentials means there is no accountability for individuals and, therefore, no audit trail that can be analysed should an incident occur.

Imprivata Enterprise Access Management with MFA removes this risk by giving care workers secure, passwordless access to electronic care records and other clinical systems with a simple badge tap. Imprivata EAM can be used with biometrics and FIDO badges for MFA, supporting a zero-trust approach and helping to provide robust identity governance. Eliminating implicit trust helps to mitigate risks from phishing, ransomware, and stolen credentials. Role-based permissions, which can be centrally managed, mean that carer workers have only the access they need to do their jobs on that day, and redundant accounts are closed down when they are no longer needed.

Challenge 4: Shared mobile devices

The use of shared mobile devices brings clinical information to the bedside/point of care. In healthcare, the growth of shared-use mobile devices is increasing, as the approach offers greater workflow flexibility, relative cost savings compared to individually assigned devices, and improved efficiency in accessing information from any location within or outside the facility or clinic. The expanding IoMT also drives mobile device adoption and optimisation, with the number of IoMT devices projected to grow 131% globally by 2026.

IoMT expansion has brought innovative healthcare solutions that enable fast, secure data transfer – for example, remote mobile access to vital signs monitoring. However, achieving efficient mobile workflows while maintaining information security and privacy is still a challenge. Care workers need to be able to access resident information and various clinical systems to provide the best care possible, but challenges like devices with small or no keyboards make frequent logins challenging for busy carers. These issues are magnified when devices are shared, often leading to the use of generic accounts or credential sharing, resulting in a lack of clear audit trails. On top of this, there is the added challenge of tracking devices and ensuring they are charged and ready for the next user.

Most access management solutions are designed for one user and one desktop or device, making usable access to shared devices a challenge. Imprivata is the leading supplier of solutions to manage the unique requirements of shared-use mobile devices in healthcare.

Imprivata provides secure, seamless access to shared mobile devices and apps. With simple authentication and a mobile-first security approach, organisations can safeguard against mobile device attacks, drive accountability, boost productivity, and maximise their mobile ROI.

Imprivata Mobile Access Management provides traceable shared access to Android devices with fast user switching, supporting bedside and on-the-go workflows. You can learn more in the case study: Surrey and Sussex Healthcare NHS Trust deploys Imprivata Mobile Device Access to enforce security and compliance for clinical mobile workflows.

Imprivata Mobile Device Access provides zero-touch provisioning and reset for iOS devices with application/catalogue delivery and certificate management for rapid swap-outs.

Challenge 5:
Compliance and audit-centralised reporting via Imprivata

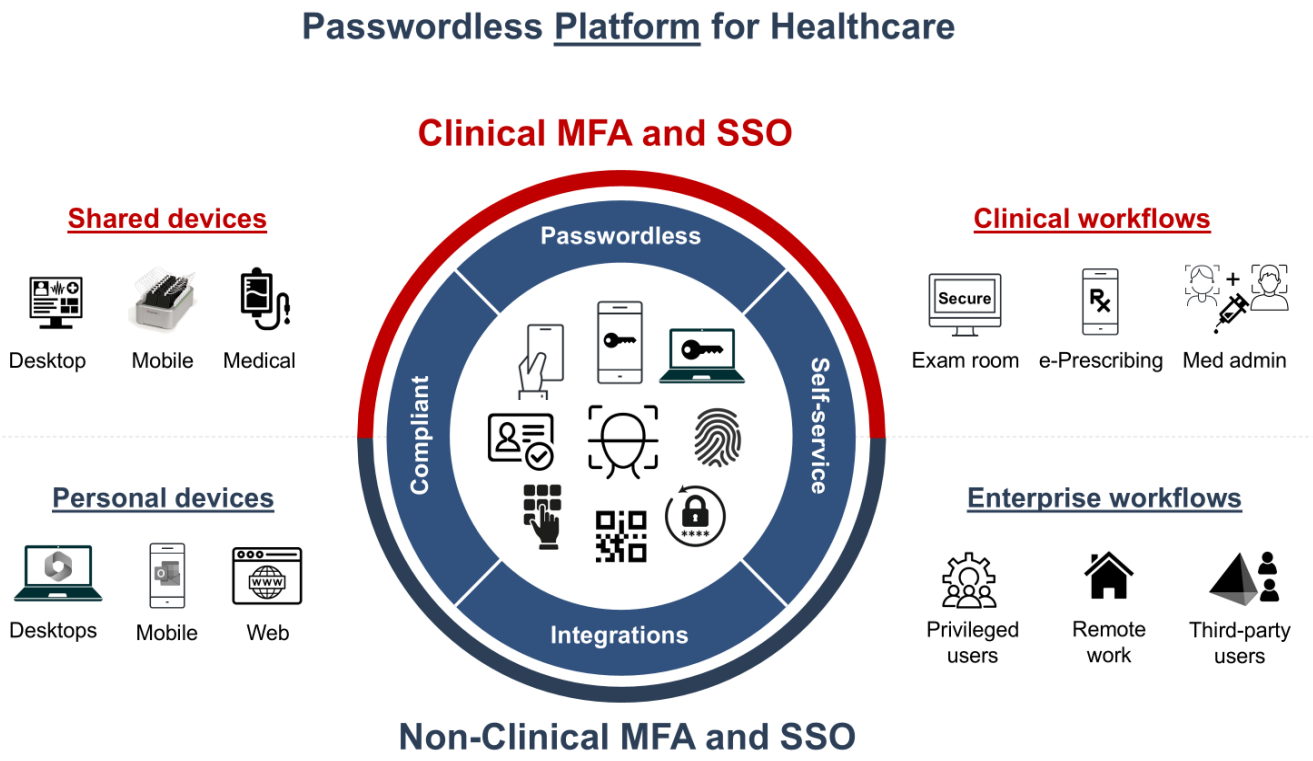
Imprivata enables aged care organisations to strike the right balance between security and friction-free access to optimise clinical workflows.

With an automated, centralised access management solution, IT can see exactly who logged in, when, and where. This enhanced visibility supports compliance. The standardisation of data collection, dashboards, and automated reports streamlines security audit preparation and compliance reporting for data privacy regulations and for AN-ACC funding returns (proving minutes of care provided per resident per day).

06

Imprivata solution architecture for aged care

Imprivata provides a single, clinical-grade access layer across desktop, virtual desktop infrastructure (VDI), and shared mobile devices. It provides deep integrations with ECR/EMR, PACS (Picture Archiving), VDI, Unified Endpoint Management (UEM), and badge and smartcard systems.



Imprivata's simple and secure access management enables aged care organisations to standardise policy, accelerate onboarding, reduce helpdesk load, and strengthen cyber and data privacy posture. All of this gives time back to care workers to focus on residents while lowering the cost to serve.

07

Case study examples with expected outcomes

Single sign-on time savings quantified

Healthcare IT teams have struggled to balance cybersecurity compliance and clinical efficiency. Each new digital system required for care delivery, such as electronic care records (ECRs), prescription services, lab portals, etc., adds another login to a busy carer's workflow. Many juggle up to 20 separate credentials per shift, according to new research published by Advances in Health Information Science and Practice (AHISP).

The peer-reviewed study was conducted by Dr. George A. Gellert MD, MPH, MPA, an epidemiologist focused on using information technology to improve public health outcomes, in association with Imprivata. The study, which covered 55 hospitals in the UK and Ireland, found that clinicians collectively lose millions of hours each year to logging in, draining both productivity and morale. The research shows that SSO has freed 3.3 million clinician hours annually, equal to 278,000 twelve-hour shifts — and generated AUS$ 109.03 million in value. On average, each facility reclaimed nearly AUS$2 million in productive time.

SUNDALE
Because we care

Sundale Ltd improves usability, efficiency and security in clinical and care workflows while enhancing data collection to meet new compliance requirements

Sundale Ltd, located in Queensland, is a community-based, not-for-profit organisation that supports the needs of its area by providing retirement communities, care centres, and in-home care support services.

Challenge – the new aged care regulation and reporting requirements for AN-ACC funding required rapid documentation to prove that 200 (rising to 215) minutes of care is provided per bed per resident per day.

Without SSO, employees had to remember multiple user IDs and passwords to access the different systems and applications used to deliver modern health and care services. There was an inconsistent user experience when accessing information across different devices and systems (laptop. desktop, Citrix, mobile, tablet), leading to staff frustration. Generic passwords were used for some devices and systems, resulting in suboptimal security and auditability.

Solution – Imprivata Enterprise Access Management for single sign-on is used across all workstations within the Sundale organisation. Imprivata Mobile Device Access facilitates access via the wide range of devices used in clinical workflows.

"Imprivata has enabled us to greatly increase data security AND improve the user experience. These two goals are no longer mutually exclusive as has been the case in the past, thanks to Imprivata."

– Lani Maxfield, Senior Systems Engineer, Sundale Ltd.

Results – Improved workflows and time savings have enhanced resident care and safety. Progress notes are now updated in real time rather than written down and entered at the end of shifts.

Due to the ease of the 'tap on/tap off' functionality and enthusiastic user acceptance, Imprivata EAM/SSO has now been extended to administrators, care and maintenance teams across the group.

"Feedback has been amazing from our carers and clinicians working across all Sundale facilities that have adopted the new solution. Everyone loves Imprivata tap on/tap off."

– Grant Morris, ICT Project Manager at Sundale Ltd.

08

Conclusion

As the aged care sector faces the ongoing challenges of meeting an ever-greater demand for its services and improving quality of care, digital transformation will deliver the operational step change required to meet these goals.

Imprivata provides supporting technology that enables healthcare organisations to deliver value across key areas.

Improved clinical quality – Fast, frictionless access to clinical information systems and e-Med systems means there is no need for workarounds, such as generic user accounts or shared credentials. Care workers can focus on what they do best, looking after residents and providing quality care.

Stronger compliance – When all carers use their own login accounts, evidence-ready audit trails and tighter access controls ensure robust compliance with information governance and clinical compliance requirements.

Cyber and privacy protection – Enforced role-based access means that care workers have access to only those systems they need to do their job on that day. This reduces the risk of lost or compromised credentials and protects privileged accounts from cybercriminals.

Operational efficiency – Significantly reduced login times have been proven to save time and reduce fatigue for care workers, leading to improved workforce utilisation as carers are able to focus more on their residents.

Future-ready digital ecosystem – Imprivata provides a scalable identity layer that supports broader digital transformation initiatives, such as patient/resident identity, privileged access security for both internal and external/trusted third-party access, and advanced IA-driven analytics that highlight abnormal access patterns and behaviours.

For more information or to book a demonstration, please call: +61 3 8844 5533

Or visit: https://www.imprivata.com/request-demo

09

Appendix – further reading

Aged Care Worker Survey 2024 Report
https://www.health.gov.au/sites/default/files/2024-12/aged-care-worker-survey-2024-report.pdf

Intergenerational Report 2023 - Australia's future to 2063
https://treasury.gov.au/sites/default/files/2023-08/p2023-435150.pdf

Aged Care Bill 2024 – Effective 1 November 2025
https://www.health.gov.au/resources/publications/guide-to-aged-care-law/overview/the-aged-care-rules

Inspector-General of Aged Care – 2025 Progress Report on Royal Commission Recommendations
https://www.igac.gov.au/resources/2025-progress-report-implementation-recommendations-royal-commission-aged-care-quality-and-safety

Aged Care Data and Digital Strategy 2024–2029 (Dept. of Health and Aged Care)
https://www.health.gov.au/resources/collections/aged-care-data-and-digital-strategy-2024-2029

Aged Care Quality and Safety Commission – Quality Standards (including Strengthened Quality Standards)
https://www.agedcarequality.gov.au/providers/quality-standards

Royal Commission into Aged Care Quality and Safety – Main Site
https://www.royalcommission.gov.au/aged-care

Recommendations: https://www.royalcommission.gov.au/system/files/2021-03/final-report-recommendations.pdf

Aged Care Workforce
https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-explained

Making a difference to patient care: The true value of access in clinical workflows
https://www.imprivata.com/uk/blog/imprivata-guest-blog-dr-gellert-value-sso-research

Sundale Ltd improves usability, efficiency and security of clinical and care workflows while enhancing data collection for new compliance requirements
https://www.imprivata.com/uk/resources/success-stories/sundale-ltd-improves-usability-efficiency-and-security-clinical-and-care

Surrey and Sussex Healthcare NHS Trust deploys Imprivata Mobile Device Access to enforce security and compliance for clinical mobile workflows
https://www.imprivata.com/uk/resources/success-stories/surrey-and-sussex-healthcare-nhs-trust-deploys-imprivata-mobile-device

StewartBrown Aged Care Financial Performance Survey Report March 2025
https://www.stewartbrown.com.au/images/documents/StewartBrown_-_Aged_Care_Financial_Performance_Survey_Report_March_2025.pdf

AHHA Digital Maturity models for Primary Health Care
https://ahha.asn.au/resource/deeble-institute-perspectives-brief-no-26-digital-maturity-models-for-primary-healthcare/

ARIIA – Sector Interpretation of Aged Care Digital Strategy
https://ariia.org.au/knowledge-implementation-hub/resources/aged-care-data-and-digital-strategy

2023-2030 Australian Cyber Security Strategy
https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

ASD – Essential Eight Explained
https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-explained

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organisations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

3977-2026_EAM-WP-ageing-australia