RACGP response to the Department of Finance consultation on verifiable credentials policy.

July 2026

RACGP

1. Introduction

The Royal Australian College of General Practitioners (RACGP) welcomes the opportunity to provide feedback on the Department of Finance's proposed Verifiable Credentials (VC) Policy.

The VC policy is not health specific but there are some key elements that will impact GPs and general practices, as general practice relies heavily on accurate and efficient verification of:

- patient identity
- Medicare eligibility and entitlements
- concession status
- healthcare provider identity and scope of practice.

Errors in these processes can lead directly to clinical safety risks, including misidentification and inappropriate care.

RACGP notes general practitioners are likely to benefit from VC implementation through the streamlining of healthcare provider identity and registration processes by enabling organisations such as Ahphra, Medicare, Services Australia and other organisations to verify practitioner credentials in real time.

Early consideration of healthcare use cases will ensure the VC ecosystem is fit-for-purpose in healthcare environments. This response focuses on key considerations for general practice, including patient safety, privacy, administrative burden and equitable access.

2. About the RACGP

The RACGP is the voice of GPs in our growing cities and throughout rural and remote Australia. For more than 60 years, we have supported the backbone of Australia's health system by setting the standards for education and practice and advocating for better health and wellbeing for all Australians.

As a national peak body representing over 50,000 members working in or towards a career in general practice, our core commitment is to support GPs from across the entirety of general practice address the primary healthcare needs of the Australian population. We cultivate a stronger profession by helping the GPs of today and tomorrow continue their professional development throughout their careers, from medical students and GPs in training to experienced GPs.

We develop resources and guidelines to support GPs in providing their patients with world-class healthcare and help with the unique issues affecting their practices. We are a point of connection for GPs serving communities in every corner of the country.

Australia's GPs see more than two million patients each week, and support Australians through every stage of life. Every year, almost nine in ten Australians visit a specialist GP for their essential healthcare, making them the most accessed health professional in the country. The scope of general practice is unmatched among health professionals. Patient centred care is at the heart of every Australian general practice, and at the core of everything we do.

3.Summary of RACGP recommendations

- Healthcare and general practice be recognised as a priority sector.
- Verifiable credential (VC) implementation in healthcare must prioritise patient safety, privacy, and equitable access to care, including maintaining non-digital pathways for patients who are digitally excluded or vulnerable.
- VC implementation must support, not replace or conflict with established safe identification practices used in general practice (and as laid out in RACGP Standards for general practices).

- VC frameworks should align with existing patient identification requirements and support safe, efficient verification processes within general practice workflows.
- Governments should prioritise nationally interoperable VC approaches that integrate with existing healthcare systems and minimise fragmentation, duplication and administrative burden.
- Any implementation must include appropriate consultation, transition support, training, and resourcing for general practice to avoid unintended workflow disruption and increased administrative burden.
- Future healthcare VC use cases should be developed in close consultation with the healthcare sector to ensure safe, practical and culturally appropriate implementation, supported by appropriate transition planning, training and resourcing for general practice.

4.Consultation response

The RACGP response addresses the matters most relevant to general practice and does not address all of the consultation sections.

Module C: Verifiers

3.3.4 VCs can reduce the need to capture and store personal data

The RACGP supports policy settings that minimise the unnecessary capture and storage of personal information, particularly where this contributes to improved privacy and data security outcomes.

The upcoming RACGP *Standards for general practices* (6th edition – scheduled for publication later in 2026) provide guidance to general practice staff and highlight that copies of identity documents must not be stored in the patient health record, as this presents a data security risk. Appropriately implemented VCs may support compliance with this requirement by enabling verification without the need to retain sensitive identity documentation.

More broadly, VCs offer a significant opportunity to strengthen privacy through selective disclosure. Rather than requiring patients to present an entire document containing information that is not relevant to the transaction, a VC could enable an individual to prove a specific attribute—such as Medicare eligibility, concession status, age eligibility, or another entitlement—without disclosing additional personal information. This data-minimisation approach reduces the amount of sensitive information collected, handled, and potentially exposed by healthcare providers, while still providing confidence in the validity of the claim being made.

However, implementation must ensure verification processes remain clinically safe, practical, and aligned with existing patient identification requirements, as per RACGP *Standards for general practices* (5th edition, C.61).

Module D: Digital wallets

3.4.1 People's choice of digital wallet should be supported

The RACGP supports consumer choice in digital wallet solutions.

However, digital credentials must not be the sole mechanism for identity verification. Not all patients have access to, or are able to use, digital technologies. It is essential non-digital pathways remain available to ensure equitable access to care, particularly for:

- older patients
- people with low digital literacy
- vulnerable or marginalised populations
- patients in rural and remote areas
- patients who do not wish to use VCs

Maintaining alternative pathways is critical to ensuring that the introduction of VCs does not create unintended barriers to healthcare access.

Module F: Privacy and consumer protection

3.6.2 Privacy and consumer protection are critical to the implementation of VCs

The RACGP strongly supports the prioritisation of patient privacy and data security.

While the Department's recognition of privacy risks (as outlined in Consultation paper – Part A, Section 6.8) is appropriate, in a healthcare context, these risks are amplified due to the sensitivity of patient information and the potential consequences of data breaches.

In alignment with upcoming RACGP *Standards for general practices* (6th edition), any VC framework must:

- align with existing healthcare privacy obligations
- minimise data exposure and unnecessary data sharing
- ensure strong safeguards against misuse, fraud, or unauthorised access and support lawful and practicable options for patient anonymity, including the use of aliases or 'disguised identities and mechanisms to change names or addresses, in sensitive circumstances such as family, domestic and sexual violence (FDSV), where disclosure of identity may pose a risk. Individuals should retain control over the use and disclosure of their verifiable credentials, with safeguards that ensure FDSV survivors can access and manage credentials safely without increasing the risk of monitoring, coercive control, or harm by perpetrators.
- incorporate cultural safety considerations for Aboriginal and Torres Strait Islander people, including accommodating community protocols around the use and display of names and images of deceased persons, in consultation with local communities where appropriate.

Protecting patient trust is fundamental to safe and effective general practice.

Module G: Voluntariness and inclusion

3.7.1 People should be able to choose whether to use a VC

3.7.2 Alternatives to VCs should remain available

The RACGP supports the principle that use of VCs must be voluntary.

It is essential that patients are not required to adopt digital credentials to access healthcare services. Consistent with the RACGP's commitment to equitable care, non-digital identification options must remain available and accessible.

Consideration should be given to circumstances where individuals are temporarily unable to access a verifiable credential, such as when they have exhausted their mobile data allowance, have a device malfunction, or face other short-term connectivity issues. While physical documents may remain available as a fallback, any delay in accessing essential services or payments could have significant consequences, particularly for people relying on government support.

The policy should also ensure verifiable credential solutions are accessible on older or lower-specification devices and do not require the latest smartphones or high levels of digital capability. Without this, there is a risk of excluding high-priority populations who may be unable to regularly upgrade their devices or access more advanced technology.

As noted above, reliance solely on digital solutions risks exacerbating health inequities and excluding some patient groups. A hybrid approach is therefore necessary to ensure inclusivity and continuity of care. General practice serves many populations at risk of digital exclusion, including older Australians, people in rural and remote areas, Aboriginal and

Torres Strait Islander people, culturally and linguistically diverse communities, and other at-risk populations, including those experiencing homelessness or family violence.

For Aboriginal and Torres Strait Islander people, it is essential healthcare remains accessible and equitable, noting that Primary care only works if everyone has access and when it can respond to populations experiencing barriers to care. Reliance solely on digital credentials risks undermining culturally safe and responsive care and exacerbating inequity, reinforcing the need for approaches that ensure inclusive access to healthcare services for all.

Module H: Interoperability and standards

3.8.1 Interoperability is essential to realise the benefits of VCs

3.8.5 Implementation requirements for nationally interoperable VCs

The RACGP emphasises that any VC solution must be interoperable with existing healthcare systems and workflows.

In particular:

- solutions must integrate seamlessly with general practice clinical information systems
- they must not introduce additional administrative burden for GPs or practice staff
- they must align with existing patient identification requirements under the upcoming RACGP *Standards for general practices* (6th edition) (the Standards)

The Standards require the use of multiple patient identifiers to confirm identity. They recognise:

- the use of digital Medicare cards as a secondary identifier (not standalone)
- that visual inspection of identification documents is sufficient
- that it is not advisable to store copies of identification

VC implementation must support, not replace or conflict with, these established safe identification practices.

Beyond patient identity verification, VCs have the potential to transform provider identity and authorisation management. GPs are frequently required to demonstrate their identity, AHPRA registration status, prescribing authority and eligibility to access government services. Verifiable credentials could enable these attributes to be validated in real time, reducing administrative burden and supporting more seamless access to systems such as PRODA.

Interoperability is a key advocacy priority for the RACGP. Fragmented or poorly integrated solutions risk increasing complexity, inefficiency and clinical risk.

Module I: Security

3.9.1 Security for VCs should follow established best practice

The RACGP strongly supports a security-first approach to the design and implementation of VCs.

Patient safety, privacy and data security must be central considerations. In healthcare settings, any failure in identity systems can have direct clinical consequences.

Security settings should:

- minimise the risk of identity fraud or misidentification
- ensure reliability and accuracy of credential verification

- support safe clinical decision-making

4.1 General questions

e) Are there any additional matters the Government should consider with respect to the proposed policy positions (for example, undesirable consequences, additional tradeoffs etc)?

The RACGP highlights the following additional considerations:

Clinical safety

VC implementation must prioritise clinical safety. Accurate patient identification is fundamental to safe care, and any changes to identity verification processes must not increase the risk of misidentification or clinical error. Healthcare interactions require strong identity verification and there are high-risk consequences if identity errors occur

Recognition of authorised representatives

General practice frequently involves interaction with:

- carers
- guardians
- enduring power of attorney
- authorised representatives

VC implementation presents an opportunity to streamline how practices identify authorised representatives and verify their authority to act on a patient's behalf. Rather than relying on the collection and storage of legal documents, credentials could carry verifiable proof of delegated authority, that can be checked instantly and securely.

Alignment with existing healthcare identifiers

Patient identification in Australia already operates within an established national framework, including the Healthcare Identifiers Service administered by Services Australia which is designed to safely exchange information across systems and protect patient privacy. While the Individual Healthcare Identifier (IHI) provides a unique national identifier, the RACGP's Standards for general practices (5th edition), and forthcoming 6th edition, do not support reliance on a single identifier as the primary means of patient identification. Instead, they require the use of multiple patient identifiers to ensure accuracy, privacy, and patient safety.

Current RACGP guidance aligns with these national arrangements, recognising the role of IHIs while embedding them within a broader multi-factor identification approach. Any VC policy should therefore align with and complement—rather than replace—this model.

Consideration should be given to how VCs interact with existing identity verification processes for both patients and providers, including scenarios where individuals must establish an IHI through existing digital identity pathways (e.g. MyGov). A VC framework that positions IHIs as the sole or primary identifier risks undermining established safety and privacy controls and would not be consistent with current general practice standards.

Multi-factor authentication (MFA)

Multi-factor authentication requirements can be burdensome for GPs and practice staff, particularly where clinicians must repeatedly obtain verification codes across multiple non-integrated systems. These interruptions add to the growing administrative and digital workload in general practice and can reduce efficiency during patient care.

From a general practitioner perspective, identity verification should support a secure single sign-on model across government and healthcare platforms to reduce repeated logins and MFA prompts while maintaining appropriate security protections.

Implementation impacts

The Government should carefully consider:

- training and support requirements
- workflow impacts in general practice
- implementation costs and system changes

Poorly implemented solutions risk increasing administrative burden, reducing efficiency, and diverting resources away from patient care. Implementation should avoid creating new administrative responsibilities for GPs and their practices, including identity proofing or credential management activities that sit outside the core role of healthcare providers.

Workforce and administrative benefits

The RACGP notes that verifiable credentials may deliver significant benefits for healthcare providers and practitioners. GPs are frequently required to verify their identity, registration and qualifications when interacting with organisations such as AHPRA, Medicare, Services Australia, professional colleges and other health services. Verifiable credentials could reduce reliance on certified copies of documents and streamline onboarding, accreditation and registration processes, particularly for practitioners working across multiple settings or jurisdictions.

The RACGP supports strong interoperability between issuers, verifiers and digital wallet providers to enable credentials to be used seamlessly across organisations.

To maximise the benefits of the framework, the Department should encourage or require agencies that undertake identity verification processes to support verifiable credentials within a defined implementation timeframe.

Cultural considerations

The development and implementation of verifiable credentials VCs must be informed by meaningful engagement with Aboriginal and Torres Strait Islander communities and peak bodies, recognising the unique cultural, historical and practical considerations associated with identity, data governance and access to services.

Particular care should be taken in relation to the use of VCs to confirm Aboriginal and Torres Strait Islander status. Across government programs and services, different approaches to identification and eligibility currently exist. For example, while some programs require formal Confirmation of Aboriginality from an Aboriginal Community Controlled Health Organisation (ACCHO) or other recognised Aboriginal organisation, eligibility for Medicare-funded Aboriginal and Torres Strait Islander health initiatives is generally based on self-identification. Linking a VC to Confirmation of Aboriginality without careful policy consideration could unintentionally alter existing eligibility arrangements and create barriers to accessing services and programs to which individuals are entitled. Decisions regarding the issuance and verification of any credentials relating to Aboriginal and Torres Strait Islander status should be guided by Aboriginal and Torres Strait Islander organisations and communities, rather than non-Indigenous entities.

Consideration should also be given to the potential risks arising from data linkage. While individual VCs may not explicitly contain information regarding Aboriginal and Torres Strait Islander status, linking credentials or datasets could enable sensitive inferences to be made about an individual. Strong safeguards are therefore needed to limit unnecessary linkage across credentials and to prevent the creation of detailed profiles that could reveal sensitive personal, cultural or health information without an individual's informed consent.

The historical experiences of Aboriginal and Torres Strait Islander peoples with identification and monitoring systems should also inform the design of the framework. For some individuals and communities, digital identity and credential systems may raise concerns regarding surveillance, control, or restrictions on access to services. These concerns should be acknowledged and addressed through culturally safe engagement, clear legislative protections, and transparent governance arrangements.

The framework should also recognise the diverse family and care arrangements that exist within Aboriginal and Torres Strait Islander communities. This includes ensuring that transitions in responsibility for credentials are appropriately managed for children moving between parental, kinship care or out-of-home care arrangements. Similar considerations will be required for people with disability, particularly those with intellectual disability, and for older people experiencing cognitive decline, balancing individual autonomy with safeguards against exploitation or misuse.

As future VC use cases are explored, their development should occur in close consultation with the healthcare sector to ensure safe, practical and culturally appropriate implementation, particularly where credentials relate to healthcare providers, organisations or professional identifiers.

Building and maintaining public trust will be critical to the successful implementation of verifiable credentials. Particular attention should be given to the concerns of Aboriginal and Torres Strait Islander peoples, who may have questions about how credential data could be used, shared, or linked across systems, including concerns about surveillance, tracking, or unintended restrictions on access to services. Strong governance arrangements, transparency regarding data use, and alignment with Indigenous Data Sovereignty principles will be essential to ensure that Aboriginal and Torres Strait Islander communities retain confidence in the system and have meaningful input into how their data is collected, managed and used.

Finally, the framework should not rely exclusively on existing identity documentation, such as birth certificates, as a prerequisite for access to services or credentials. Alternative pathways should be available to ensure that individuals who do not possess, or cannot readily obtain, foundational identity documents are not excluded from healthcare, government services or other essential supports.

5.Conclusion

The RACGP supports the potential role of verifiable credentials in strengthening privacy, security and efficiency. However, their implementation in healthcare must be carefully designed to ensure:

- patient safety is maintained
- privacy is protected
- administrative burden is minimised
- systems are interoperable
- access to care remains equitable

We thank you for the opportunity to provide input into the Verifiable Credentials Policy. The RACGP looks forward to continued engagement to ensure any future implementation supports safe, high-quality general practice care.

For any enquiries regarding this submission, please contact Joanne Hereward, Program Manager – Practice Management and Technology via joanne.hereward@racgp.org.au.