Regulating the use of healthcare identifiers in health technology

Medical Technology Association of Australia

submission

Friday, 9 October 2026

Contact	Andrew Wiltshire, Head of Digital Health
Email	awiltshire@mtaa.org.au

Medical Technology Association of Australia Ltd
Level 4, 97 Waterloo Rd, Macquarie Park NSW 2113
P: (02) 9900 0600 | E: mtaa@mtaa.org.au

About MTAA

The Medical Technology Association of Australia (MTAA) is the peak body representing companies in the medical technology industry. MTAA's membership spans Australian start-ups through to global MedTech leaders. Members develop, manufacture, supply and support technologies used in the diagnosis, prevention, treatment and management of disease and disability.

The technologies supplied by MTAA members range from familiar products such as syringes and wound dressings to implantable devices, diagnostic imaging equipment, connected medical devices, remote patient monitoring technologies, software as a medical device and digital therapeutics. MTAA members also provide healthcare professionals with education, training and technical support to promote safe and effective use.

Executive summary

MTAA supports the policy objective of enabling safer and more reliable matching of health information generated or managed by consumer-facing health technology. A nationally consistent pathway for eligible health technology providers to use Individual Healthcare Identifiers (IHIs), with informed consent and appropriate safeguards, can support connected care, remote monitoring and more reliable information exchange.

The proposed framework should, however, be refined so that responsibility is allocated to the entity that actually provides the relevant electronic service and relies on the new IHI authorisations. Manufacturing, sponsoring, distributing or supplying a medical device or medical software should not, by itself, make an organisation a health technology provider (HTP).

A workable framework must also avoid duplicating Therapeutic Goods Administration (TGA) assessment, provide practical rules for IHI validation in continuous and high-volume workflows, distinguish withdrawal of consent to use an IHI from clinical recordkeeping and safety obligations, and provide adequate implementation time after final conformance specifications and test services are available.

MTAA'S CENTRAL REQUEST

Proceed with the consent-based expansion of IHI use, subject to clear entity-level scope, proportionate and reusable conformance assurance, workable validation and consent rules, lawful retention for safety and regulatory purposes, internationally aligned UDI design, and staged implementation before enforcement.

Medical Technology Association of Australia Ltd
Level 4, 97 Waterloo Rd, Macquarie Park NSW 2113
P: (02) 9900 0600 | E: mtaa@mtaa.org.au

Priority recommendations

- Clarify in regulations or authoritative guidance that manufacture, sponsorship, distribution or supply of a medical device or medical software does not itself create HTP status.
- Publish worked examples that identify the HTP in manufacturer, platform, healthcare-provider, distributor and outsourced-service arrangements, including hybrid models.
- Limit HI conformance to IHI-specific risks and recognise existing TGA, security, quality-management and other equivalent assurance evidence.
- Define practical IHI validation rules for continuous monitoring, automated alerts, scheduled transfers and outages, including caching and risk-based revalidation.
- Specify consent requirements for ongoing services, representatives, minors, changed care teams and multi-party data flows, and distinguish IHI consent from consent to treatment and clinical-record retention.
- Permit continued retention of the minimum necessary IHI or linkage record where required for patient safety, recalls, adverse-event investigation, post-market surveillance, cybersecurity, audit or other legal obligations.
- Use globally harmonised UDI standards and authoritative TGA-managed data, avoiding a separate or duplicative identifier repository.
- Apply version control, consultation and transition periods to updated conformance requirements rather than immediate dynamic compliance.
- Provide at least 12 months from publication of final specifications and availability of operational test services to substantive enforcement, with proportionate support for SMEs and local subsidiaries.
- Use graduated, risk-based enforcement and procedural fairness before suspension or removal from the HI Conformance Register.

1. Overall position and policy objective

MTAA supports expanding the lawful use of IHIs where this improves patient matching and enables health information generated outside traditional care settings to be associated with the correct person. The reform is particularly relevant to remote patient monitoring, connected devices, digital therapeutics, patient-engagement services and other technologies that communicate health information between consumers, providers and health administration entities.

The policy objective should be pursued through controls that are technology-neutral, proportionate to risk and clear about organisational responsibility. The framework should protect privacy and matching accuracy without creating a second product-approval regime or imposing obligations on entities that do not provide the relevant electronic service.

2. Scope and identification of the responsible HTP

The central implementation issue is identifying which entity is the HTP in contemporary service models. A connected-care pathway can involve a manufacturer, Australian sponsor, distributor, cloud or platform operator, healthcare provider, clinical-service company and integration provider. These parties may exercise different levels of control over the electronic service, consent, IHI handling and disclosure of associated information.

The framework should confirm that an entity is directly subject to HTP requirements only where it provides the relevant electronic service, meets the statutory definition and relies on the new authorisations to collect, use or disclose an IHI. Product manufacture or supply alone should not be sufficient.

RECOMMENDED SCOPE TEST

Guidance should ask: Who provides the electronic service? What is its sole or primary purpose? Who determines the purpose and means of the relevant IHI handling? Which entity relies on the new authorisation? Who holds the direct relationship with the healthcare recipient and operates consent withdrawal?

Worked examples should address at least:

a manufacturer that supplies a connected device while a hospital operates the monitoring service;
a multinational platform with an Australian sponsor or distributor but centralised overseas service operations;
a digital therapeutic supplied to a healthcare provider under a service agreement;
a clinical-service company using a third-party technology platform;
a hybrid service combining provider-facing clinical software and a consumer-facing application; and
a healthcare provider or health administration entity that receives device-generated information from several technology suppliers.

3. Registration, connection and conformance

MTAA accepts that registration, connection and conformance can be appropriate prerequisites for organisations relying on the new IHI authorisations. The requirements should be confined to assurance that is necessary for accurate, secure and lawful IHI handling.

The conformance process should recognise substantially equivalent evidence already generated for TGA regulation, quality management, cybersecurity, privacy and service assurance. Requiring the same organisation to repeat product or organisational assessments in a separate HI process would add cost without necessarily reducing IHI-specific risk.

The Department and HI Service operator should publish a clear conformance map showing each control, the evidence accepted, responsible assessor, renewal trigger

Medical Technology Association of Australia Ltd
Level 4, 97 Waterloo Rd, Macquarie Park NSW 2113
P: (02) 9900 0600 | E: mtaa@mtaa.org.au

and relationship to existing assurance. Reusable evidence should be accepted across customers and deployments where the control and system boundary are materially equivalent.

RECOMMENDATION

Adopt an evidence-reuse model: assess only the IHI-specific gap after recognising relevant existing evidence, rather than repeating a full assessment of the medical device or broader digital service.

4. Relationship with TGA regulation

Where health technology is, or includes, a medical device, evidence of relevant TGA status may be a useful conformance input. It should not become a second assessment of safety, performance, intended purpose or quality-management matters already addressed through therapeutic-goods regulation.

The framework should distinguish the regulated medical device from the broader electronic service. Depending on the delivery model, the legal manufacturer or sponsor of the device may not operate the service that collects, uses or discloses the IHI. Conversely, an organisation may operate an in-scope service using technology that is not itself a medical device.

Guidance should therefore explain what evidence is required, from whom, and how it will be treated where the device, platform and service operator are different entities. Any change-notification or ongoing-conformance requirement should focus on changes material to IHI handling rather than every product update.

5. IHI validation and service availability

The requirement to validate an IHI before disclosing associated information should be designed for both episodic and continuous data flows. Validation before every individual data transmission may be impractical for remote monitoring, automated alerts or scheduled bulk transfers and could introduce latency or failure points without a proportionate improvement in matching accuracy.

The final framework should specify:

- events that trigger initial validation and revalidation;
- permitted caching periods and controls;
- how identity or demographic changes are handled;
- outage, disaster-recovery and emergency arrangements;
- processing of queued data once the HI Service becomes available;
- logging, audit and exception-management requirements; and
- risk-based treatment of high-frequency, low-change monitoring workflows.
- The approach should preserve patient safety. An unavailable validation service should not automatically prevent a clinically necessary alert or communication where appropriate fallback controls can maintain identity confidence and the disclosure is recorded for later reconciliation.

Medical Technology Association of Australia Ltd
Level 4, 97 Waterloo Rd, Macquarie Park NSW 2113
P: (02) 9900 0600 | E: mtaa@mtaa.org.au

6. Consent, withdrawal and multi-party workflows

MTAA supports clear and informed consent for HTP use of IHIs. Consent requirements must nevertheless be operationally workable for ongoing monitoring and multi-party care pathways. Guidance should address the content, duration, renewal and withdrawal of consent, including representatives, minors, changes in capacity, changed care teams and multiple authorised recipients.

The framework should distinguish consent to use an IHI from consent to treatment, participation in a service, use of broader health information and retention of clinical or safety records. Withdrawal of IHI consent should stop future reliance on the IHI authorisation, but should not be interpreted as requiring deletion of information that must lawfully be retained or that is necessary to preserve the integrity of a clinical, audit, safety or regulatory record.

Where several organisations participate in a service, the framework should define responsibility for communicating withdrawal and the minimum information needed to propagate it safely. It should support auditable status messages and clear effective dates without requiring disclosure of unnecessary personal information between parties.

7. Retention, deletion and safety obligations

MTAA supports data minimisation and cessation of IHI use when consent expires or is withdrawn. The regulations and conformance requirements should expressly accommodate retention required for patient safety, complaint and adverse-event investigation, recalls and field safety actions, post-market surveillance, cybersecurity, fraud prevention, audit and other legal obligations.

A proportionate approach would permit retention of the minimum necessary IHI or linkage record, subject to restricted access, purpose limitation, security, logging and defined review. The framework should also address backups, immutable audit logs and distributed systems, where immediate physical deletion may be technically infeasible or may undermine security and record integrity.

RECOMMENDED SAFEGUARD

Allow secured, beyond-use retention where the record is no longer used for the original service but must be preserved for a defined safety, integrity or legal purpose. Require documented justification, access restriction and periodic review.

8. UDI and device traceability

MTAA supports exploring an optional association between an available Unique Device Identifier (UDI), the IHI and relevant health information where this delivers a clear clinical, traceability or post-market benefit. The design should use globally harmonised UDI standards and authoritative TGA-managed data and should not create a parallel identifier or duplicate master-data entry.

The Department should define the use case before determining the data fields. UDI-DI, production identifiers, serial number, lot or batch and software version serve different purposes and have different privacy, accuracy and lifecycle implications. Not every field will be necessary or appropriate for every technology or disclosure.

Any implementation should clarify who records and corrects the device information, how replacements and software updates are represented, how authoritative data are referenced, and whether the association is stored centrally or exchanged only as part of a defined clinical message.

9. Implementation, transition and impact on SMEs

The intended commencement date creates a substantial implementation risk if final regulations, conformance requirements, technical specifications, test environments and onboarding processes are not available sufficiently early. Affected organisations may need to determine legal roles, redesign consent and withdrawal workflows, build or modify interfaces, complete assurance activities, update contracts and privacy materials, train staff and coordinate with healthcare-provider customers.

MTAA recommends at least 12 months between the availability of final specifications and operational test services and substantive enforcement. Updated conformance requirements should be versioned, consulted on and accompanied by transition periods based on materiality and risk.

SMEs, start-ups and local subsidiaries may face disproportionate fixed costs. Implementation support should include plain-language role guidance, worked architectures, standard consent and contract clauses, test tooling, a conformance evidence matrix, help-desk support and proportionate fees.

10. Enforcement and procedural fairness

Enforcement should be graduated and risk-based. Maximum civil penalties should be reserved for serious, repeated or deliberate non-compliance, particularly conduct that creates material privacy or patient-matching risk. The framework should support education, corrective action plans, warnings and enforceable undertakings before punitive action where the issue is remediable and there is no serious or intentional harm.

Suspension or removal from the HI Conformance Register may interrupt services and affect patients and healthcare providers. Decisions should therefore include notice, reasons, an opportunity to respond, proportionate remediation periods, review rights and continuity arrangements where immediate cessation would create a greater safety risk.

11. Recommended implementation package

Before commencement, MTAA recommends that government publish a coordinated implementation package containing:

- final regulations and an explanatory statement;
- authoritative scope and entity-responsibility guidance with worked examples;

Medical Technology Association of Australia Ltd
Level 4, 97 Waterloo Rd, Macquarie Park NSW 2113
P: (02) 9900 0600 | E: mtaa@mtaa.org.au

- a conformance control and evidence-reuse matrix;
- technical specifications, test environments and onboarding dates;
- validation, caching, outage and reconciliation rules;
- consent and withdrawal guidance with model wording and multi-party status flows;
- retention and deletion guidance covering safety, audit, backups and immutable logs;
- UDI use cases and data architecture aligned with TGA-managed sources;
- a versioning and transition policy for future requirement changes; and
- a compliance and enforcement policy including procedural protections.

12. Direct response to the consultation questions

The recommendations below are confined to the safeguards and implementation matters raised by the consultation paper: HTP scope, registration and connection, conformance, TGA evidence, UDI, IHI validation, consent, retention and destruction, ongoing compliance, and the proposed civil penalty.

Impact on HTPs and MTAA members: Members that provide an in-scope electronic service and rely on the new IHI authorisations may need to determine legal roles, register and connect with the HI Service, demonstrate conformance, implement validation and consent controls, update contracts and privacy materials, and support ongoing compliance. The impact will be disproportionate where responsibility is unclear in multi-party models or where existing assurance evidence cannot be reused. Manufacture, sponsorship, distribution or supply alone should not create HTP status unless the entity also meets the statutory definition and relies on the new authorisation.

Reasonableness of the proposed requirements: Registration, connection, conformance, validation, consent and cessation of use are reasonable in principle. They should be proportionate to IHI-specific risk, distinguish the medical device from the electronic service, accommodate continuous monitoring and outages, and preserve records that must be retained under applicable law or for defined safety purposes.

Problems, risks, gaps or concerns: The main gaps are allocation of responsibility in multi-party services; the form and reuse of evidence of relevant TGA approval; validation frequency, caching, outages and reconciliation; consent duration and withdrawal across participating entities; treatment of backups, audit logs and legally required records; versioning of updated conformance requirements; and readiness of specifications, test services and onboarding processes.

Penalty provision: A civil penalty provision may be appropriate. Application of the proposed maximum of 50 penalty units should be reserved for serious, repeated or deliberate contraventions. Technical, transitional or readily remediable failures that do not create material privacy or patient-matching risk should ordinarily be addressed through proportionate compliance action and procedural fairness.

Other safeguards or regulatory options: Government should publish authoritative role guidance and worked examples; a conformance evidence map; practical validation, caching, outage and reconciliation rules; consent and withdrawal

guidance; retention and destruction guidance; and versioning and transition arrangements. MTAA recommends at least 12 months from publication of final specifications and availability of operational test services to substantive enforcement, based on the implementation activities identified in this submission.

12.1 TGA perspective

The consultation paper proposes that conformance require evidence of relevant TGA approval where the technology is or includes a medical device. MTAA supports that proposal, provided the conformance process specifies the evidence required, identifies which entity supplies it where the manufacturer, sponsor and service operator differ, and avoids reassessing matters already addressed through therapeutic-goods regulation. Ongoing notifications should focus on changes material to IHI handling, validation, consent, security or disclosure.

The paper also proposes consideration of an optional UDI field. MTAA supports this in principle, provided the use case, relevant UDI data element, authoritative source, correction responsibility, privacy controls and lifecycle arrangements are defined before implementation. The design should align with the TGA UDI framework and avoid a duplicative device-identifier repository.

12.2 Clinician and patient-safety perspective

More reliable patient matching can support remote monitoring and connected care. Validation controls should not create a single point of clinical failure. Conformance requirements should identify when initial validation and revalidation are required and provide controlled arrangements for outages, queued information, clinically necessary alerts, audit logging and later reconciliation. These are implementation details of the validation proposal, not a request to broaden the statutory authorisation.

12.3 Consumer perspective

Consumers should receive accessible information about why an IHI is needed, who will handle it, the authorised purpose, consent duration, withdrawal, and any records that must remain because of applicable legal retention requirements. Withdrawal should stop future use under the consent-based authorisation and be propagated across participating entities, while the regulations should preserve the consultation paper's express qualification for applicable legal retention requirements.

Conclusion

MTAA supports a trusted national framework that enables eligible health technology providers to use IHIs with consent and appropriate safeguards. Clear identity matching can strengthen connected care and the safe exchange of information generated by remote monitoring, connected devices, digital therapeutics and other consumer-facing technologies.

The success of the reform will depend on precise scope, practical allocation of responsibility, reuse of existing assurance evidence, workable validation and consent rules, recognition of safety and legal retention, and sufficient implementation time.

With these refinements, the framework can protect healthcare recipients while enabling scalable and interoperable digital health services.

MTAA welcomes continued engagement with the Department of Health, Disability and Ageing, the Australian Digital Health Agency, Services Australia, the TGA and other relevant stakeholders on the regulations, conformance design and implementation arrangements.

References

[1] Australian Government Department of Health, Disability and Ageing, Regulating the use of healthcare identifiers in health technology: Consultation paper, September 2026.

[2] Healthcare Identifiers Act 2010, including amendments scheduled to commence on 1 February 2027.

[3] Medical Technology Association of Australia, MTAA Member Consultation: Healthcare Identifiers in Health Technology (Revised), September 2026.

[4] Medical Technology Association of Australia, Privacy Reform: Consultation on Exposure Draft Legislation, September 2026.