Submission to the "Charting New Horizons: Horizon 2" Policy Discussion Paper for the Australian Cyber Security Strategy (2025)

Health Information Sharing and Analysis Center (Health-ISAC) is the global, non-profit information sharing and analysis center dedicated to the health sector. With more than 1,000 organizations worldwide operating in 140 countries, including healthcare providers, pharmaceutical and biotechnology companies, medical device manufacturers, insurers, and supporting services, Health-ISAC enables trusted, cross-border collaboration for more than 15,000 health sector professionals to strengthen patient safety and the resilience of health systems.

Health-ISAC maintains a 24/7/365 intelligence-sharing platform, offers sector-specific threat analysis, coordinates incident responses, and hosts workshops and summits globally. Health-ISAC collaborates with governments worldwide to improve cyber resilience and bolster health sector defences, including in North America, Europe, and the Asia-Pacific.

Our mission is simple but critical: to empower trusted relationships in the global Health Sector to prevent, detect, and respond to cybersecurity and physical security events so that Members can focus on improving health and saving lives.

Health-ISAC's Commitment to Australia and the Region

Health-ISAC has a long-standing and expanding commitment to Australia and the broader Asia-Pacific health ecosystem. Health-ISAC has sixteen health sector member organizations with headquarters in Australia and is actively expanding local support. In September 2025, Health-ISAC is adding two additional Cyber Threat Intelligence Analysts to our APAC operations, and in Q1 2026 we will add an APAC Operations Director to deepen engagement with governments and industry.

Health-ISAC convenes regular regional workshops across Asia-Pacific to build trust, improve threat intelligence exchange, and strengthen sectoral resilience. In Australia specifically, we held a regional workshop in Melbourne in June 2025, which brought together public and private stakeholders from across the health sector. The workshop built on earlier engagement and will continue as part of our APAC program in 2026 and beyond. These sessions provide a practical platform for Australian providers to exchange insights with their peers, government, and global members.

Health-ISAC has also made long-term investments in bringing its flagship summits to Australia. We hosted the 2024 APAC Summit in Victoria, convening health sector security leaders from across Asia-Pacific. Health-ISAC will continue to host future events in Australia, including a regional workshop in 2026, and the Health-ISAC APAC Summit held on the Gold Coast in 2027, underscoring our sustained commitment. The 2027 APAC Summit will also include a tabletop exercise (TTX), building on an annual program we started in 2019, Health-ISAC's "Hobby" Exercise Series. Hobby, named after the first head of the US Department of Health, Education and Welfare, involves private-sector entities and their government partners in a TTX

that focuses on cybersecurity and physical security challenges, as well as the best ways to respond to widespread incidents.

Response to Consultation Question 28

"What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low-maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?"

Health-ISAC commends the Australian Government for recognising that a world-class threat sharing and blocking ecosystem is central to Horizon 2. In our experience, success depends on three elements: meaningful government-to-industry engagement, participation that extends beyond large providers, and close alignment with international networks.

The question of the creation of ISACs requires careful consideration. While creating uniquely Australian ISACs may appear attractive from a sovereignty perspective, experience shows that such efforts often duplicate resources, fragment trust frameworks, and narrow the intelligence pool. Cyber threats are inherently global; ransomware campaigns, phishing operations, and supply chain compromises rarely respect borders. Sovereign ISACs risk isolating Australian stakeholders from richer global data flows, slowing detection of cross-border campaigns and limiting access to subject matter experts already operating in existing ISACs. The risk is especially acute in the health sector, where the largest healthcare organisations in the world already participate in Health-ISAC's global network. Attempting to create a parallel, sovereign-only model would disconnect Australian stakeholders from the intelligence these global entities rely upon to protect patients and systems.

A more cost-efficient and sustainable model is to support access for Australian entities into mature international ISACs that are committed to establishing a local presence, while also ensuring Small to Medium-sized Businesses (SMBs) and lower-maturity organisations have clear information on how to participate and benefit. By plugging these organisations into the existing ISAC models, which have committed to operating in Australia and understanding the local threat and regulatory environment, they can benefit from mature information security communities with proven economies of scale in intelligence sharing and capacity-building, rather than being left isolated against sophisticated threat actors.

Health-ISAC stands ready to partner with the Australian Government and health sector stakeholders to achieve these outcomes. Our commitment to Australia is longstanding, growing, and anchored by local staff, regular workshops, future summits and enduring engagement with the health community.