Medibank Private Limited: Submission on Subordinate Legislation to the Cyber Security Act and SOCI Act

February 2025

Medibank Private Limited

14.02.2025

Contact: Simon.Howe@medibank.com.au

About Medibank Private Limited

We're a health company working to create Better Health for Better Lives by providing the best health and wellbeing experience for people across Australia. Building upon our 49-year history as one of Australia's leading health insurers, our Medibank and ahm brands now support millions of customers to manage their health and wellbeing through personalised products and services. We're investing in preventative health and reimagining healthcare to give people greater choice, better access, and more control over their care. We're partnering with doctors, hospitals and governments to deliver care in new ways – and growing and developing new health services through our Amplar Health business. We're also working together to drive change within Australia's healthcare system to help ensure it can support our generation and those to come.

Feedback on the proposed Rules

Medibank Private Limited (Medibank) welcomes the opportunity to provide feedback on the Consultation on Subordinate Legislation to the *Cyber Security Act 2024* and *Security of Critical Infrastructure Act 2018* (SOCI Act) published by the Department of Home Affairs (Department).

Please note that we have restricted our response to those Rules on which we had specific feedback, as outlined below. If you have any questions relating to our submission, please contact us using the details provided on the cover page.

1. Cyber Security (Cyber Incident Review Board) Rules 2024

- **Part 2, Division 2, Section 8 - Matters Board must consider when prioritising referrals and reviews**

Medibank supports the proposed considerations for prioritising referrals and reviews. However, we submit that the availability and capacity of the impacted entity should also be considered by the Board when prioritising referrals and reviews. Significant regulatory burden and stress is placed on entities following a cyber security incident even after the immediate response has ended. Extensive resources are likely to be dedicated to containing the incident, forensic investigation into the cause of the incident and system vulnerabilities, necessary changes to systems and controls, and responding to inquiries from regulators and stakeholders (e.g., customers, suppliers, shareholders). These factors must be considered and balanced against the security and scale of the cyber security incident before imposing on an entity the additional burden of a review.

- **Part 2, Division 2, Section 10 - Timing of reviews—non-interference with investigations etc.**

The note to Part 2, Division 2, Section 10 refers to section 46(2)(b) of the *Cyber Security Act 2024*, and states that *'[a] review may only be conducted after the incident or series of incidents, and the immediate response, has ended'*. It is unclear how this requirement will be interpreted in practice. Steps taken to contain and resolve a cyber incident may extend over a prolonged period of time, as it may involve conducting investigations, notifying relevant parties, securing systems, and addressing any system vulnerabilities. Medibank considers that the timing of reviews should not interfere with these processes, and requests that further clarification be provided in the Rules on when an immediate response to a cyber incident will be considered to have ended.

- **Part 2, Division 3, Section 13(1)(b) – Eligibility for appointment as a standing member of the Board**

Medibank supports the eligibility criteria listed in section 13(1)(b). However, the experience and qualifications outlined are listed as being alternatives. This could result in the composition of a Board without any relevant expertise in cybersecurity, which is critical to the effectiveness of the body. We consider that all appointments must have at a minimum, a qualification in the field of cybersecurity or have experience in cybersecurity related matters. Alternatively, the rules should require that there be a minimum number of members on the Board with qualifications in the field of cybersecurity or experience in cybersecurity-related matters.

- **Part 2, Division 4, Section 22(3)(b) – Appointments to Expert Panel**

Medibank reiterates its comments on Part 2, Division 3, Section 13(1)(b) above in relation to the eligibility requirements for appointments to the Expert Panel.

Draft review report

Section 51(4) of the *Cyber Security Act 2024* states that the Board *may* give a draft review report, or an extract of the draft review report to another entity:

- if the Board considers it appropriate to give the entity an opportunity to make submissions on the draft review report or the extract; or
- for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.

Medibank considers that impacted entities should be provided an opportunity to review and comment on the draft report in the following circumstances given the report will be published:

- if the report contains confidential, commercially sensitive, or personal information provided by the entity;
- if the report contains adverse findings relating to the entity;
- if the report contains recommendations requiring the entity to make changes to its operations or systems.

Medibank requests that clarification be provided in the Rules on when the Board must provide an impacted entity with the opportunity to review and make submissions on the draft report.

2. Cyber Security (Security Standards for Smart Devices) Rules 2024

Schedule 1, Part 1, section 1 defines 'cryptographic key' to mean '*data used to encrypt and decrypt data*'. Medibank notes that a cryptographic key is more widely understood to be a key or code used to encrypt and decrypt **data**.