Private Healthcare Australia
Better Cover. Better Access. Better Care.

Engagement on critical infrastructure reforms

January 2022

Contact:

Ben Harris
Director Policy and Research
0418 110 863 or ben.harris@pha.org.au

About PHA

Private Healthcare Australia (PHA) is the Australian private health insurance industry's peak representative body that currently has 22 registered health fund members across Australia and collectively represents 97% of people covered by private health insurance. Over 14 million Australians hold private health insurance.

Response to asset definitions and risk management program rules

Thank you for the opportunity to comment on the draft asset definitions and risk management program rules for *Security of Critical Infrastructure Act 2018* (the SOCI Act).

Private health insurance is a heavily regulated industry, with compliance and reporting requirements with a range of agencies including the Australian Prudential Regulatory Authority (APRA), the Australian Competition and Consumer Commission (ACCC), departments of health, Services Australia and various other agencies. We note that the proposals will impose additional regulatory burden on registered health funds. This burden can be minimised through considering the following issues.

Duplicated regulation

Private Health Insurers already have existing reporting requirements to APRA under Prudential Standard CPS 234 on Information Security (CPS 234). CPS 234 outlines requirements for private insurers to maintain information security capability.

CPS 234 requires a private health insurer to, among other things:

- maintain an appropriate information security policy framework
- identify and classify its information assets by criticality and sensitivity
- implement information security controls and test their effectiveness
- have robust incident management mechanisms
- notify APRA as soon as possible, and in any case, no later than 72 hours, after becoming aware of an information security incident that:
    - materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or
    - has been notified to other regulators, either in Australia or other jurisdictions,
- notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which it expects it will not be able to remediate in a timely manner.

These obligations are duplicated by Parts 2A and 2B of the Act. The term 'critical insurance asset' should be removed from the list of specified assets in Rule 5(1) where these bodies hold similar obligations under CPS 234, as there is already an established process for APRA-regulated entities to notify an appropriate regulator (APRA) when a material information security incident (or weakness) occurs.

The rules should be amended to require APRA to notify the Department of Home Affairs under an information-sharing protocol when an incident is notified. If this is not possible, then there should be changes to enable compliance with the SOCI Act by lodging a notification that is made to APRA in accordance with CPS 234.

Definitions

The current application to all assets of a Private Health Insurer is extremely broad. Currently, it is proposed that any 'asset' owned or operated by a Private Health Insurer and used in connection with the health insurance business will be relevant. 'Asset' is defined so broadly in the Act as to include, after a list specifying items such as systems, networks, facilities, data and premises, or 'any other thing'.

The Act says that the impact is significant only if the asset is used in connection with the provision of essential goods or services, and the incident materially disrupts the availability of those goods or services. However, neither the Act nor the draft Rules specify what an essential good or service is. It will be challenging to fit the concept to the business of Private Health Insurance, and although the Explanatory Memorandum to the Act said the Department would provide guidance and support to industry to assist it to identify what a significant impact would be in 'different sectoral contexts', there was nothing in the correspondence to industry or draft Rules that would assist Private Health Insurers.

Similarly, guidance should be provided on the application of the term 'relevant impact' in s.30BD of the Act, and the situations in which there is an impact on the 'availability', 'integrity', 'reliability' and 'confidentiality' of an asset. In terms of confidentiality, the current drafting in the Act would impose more onerous and wider reporting requirements than the existing notifiable data breach reporting requirements under the *Privacy Act 1988* or under CPS 234. it would be unreasonable for any impact on the confidentiality of any information contained in a Private Health Insurer's database to be reportable even where the impact of the loss of the confidentiality is minimal (for example, does not meet the threshold for reporting to the Office of the Australian Information Commissioner).

Notification of incidents should only be required where material in terms of impact on policyholders (and other key stakeholders) or the services provided by private health insurers. Failure to do this is likely to result in affected private health insurers incurring significant costs in implementing systems to report on immaterial incidents or risk breaching the Act. In addition, reporting of immaterial incidents would flood the system and not allow regulators to get a clear picture of threats faced by industry in a timely manner.

As proposed, the breadth of the definitions and the way it is used across all obligations imposed under the Act will provide significant implementation challenges to meet obligations in a way that is sensible and cost effective.

The Rules should expand on what the applicable threshold for 'material disruption of the availability of essential goods/services' is, and align with the materiality test under CPS 234.