Mail GPO Box X2221 Perth WA 6847
Office Level 4, 100 Stirling Street Perth WA 6000
Call 1300 13 40 60
Fax (08) 9328 3345
Email info@hif.com.au

Your health
Your choice

7 June 2018

Ms Heidi Richards
General Manager – Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
Email: PolicyDevelopment@apra.gov.au

Dear Ms Richards

Information Security Management: A New Cross-Industry Prudential Standard

Health Insurance Fund of Australia Limited (**HIF**) has conducted a review of the documents released by the Australian Prudential Regulation Authority (**APRA**) on 7 March 2018, as part of its consultation package on Information Security Management (**Consultation Package**).

HIF is a member of Private Healthcare Australia (**PHA**). This advice is independent of any advice APRA may receive from PHA.

HIF is encouraged by APRA's proposal to strengthen information security resilience across all APRA-regulated industries, in order to better address the evolving nature of information security matters, through the introduction of Prudential Standard 234 Information Security (**CPS 234**).

HIF would like to comment on the following aspects of the proposed requirements as outlined in the Consultation Package:

Policy Framework

HIF notes APRA's requirement for an APRA-regulated entity to maintain an information security policy framework commensurate with its exposure to vulnerabilities and threats. HIF also notes that APRA is seeking industry views on guidance topics that would assist with the understanding and implementation of CPS 234.

HIF would therefore like to seek APRA's guidance regarding an appropriate information security framework that should be considered for implementation by APRA-regulated entities. For example, International Standards Organisation (**ISO**) 27000, Control Objectives for Information and Related Technology (**COBIT**) or US National Institute of Standards and Technology (**NIST**). Alternatively, it would be appreciated if APRA could share its views regarding the minimum requirements that must be considered by an APRA-regulated entity upon implementation of the proposed information security policy framework.

Information Asset Identification and Classification

HIF notes APRA's requirement for an APRA-regulated entity to classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. HIF is pleased to note that APRA plans to provide APRA-regulated entities with guidance on information asset classification in its revised Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology (**CPG 234**).

As part of this guidance, HIF requests that APRA consider implementing standardised information asset classification categories per APRA-regulated industry, which will assist in ensuring consistency in the

application of information asset classification categories across industries that process and maintain similar information assets.

Incident Management

HIF notes APRA's requirement for an APRA-regulated entity to maintain information security response plans to respond to information security incidents in a timely manner and further, that APRA requires an APRA-regulated entity to annually confirm that its information security response plans are effective.

HIF believes that it will need to engage the services of an independent third party to conduct scenario testing in order to annually confirm the effectiveness of HIF's information security response plans. This will, in all likelihood, introduce additional compliance costs on HIF. We consider the compliance costs associated with the required scenario testing may be ~$30k - $50k per annum, which fees we regard as neither immaterial nor material.

Internal Audit

CPS 234, Internal Audit, paragraph 31 states: *"An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance)."*

Controls effectiveness testing is also mentioned under two other paragraphs within CPS 234, as follows:

Implementation of Controls, paragraph 21 states: *"Where information assets are managed by a related party or third party, an APRA-regulated entity must evaluate the design and operating effectiveness of that party's information security controls."*

Testing Control Effectiveness, paragraph 26 states: *"An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program."*

It is unclear from CPS 234 whether the control effectiveness testing referred to in paragraphs 21 and 26 above can also be performed by an outsourced Internal Audit arrangement, or whether APRA expects an appropriately skilled and functionally independent internal department to perform the testing referred to in paragraphs 21 and 26.

HIF therefore requests clarity regarding APRA's expectation with regard to who will be required to perform the control effectiveness testing in each of the paragraphs mentioned above.

HIF believes that the additional costs to be incurred as a result of increased internal audit activity will not have a material financial impact on HIF.

APRA Notification

HIF notes APRA's requirements for an APRA-regulated entity to:

a) Notify APRA as soon as possible, but no later than twenty-four (24) hours, after experiencing a material information security incident; and
b) Notify APRA as soon as possible, but no later than five (5) business days, after identifying a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.

With regard to paragraph (a) above, HIF believes it would be reasonable for APRA to align its notification requirements with those of the European Union General Data Protection Regulation (**EUGDPR**) i.e. seventy-two (72) hours, in order to relieve the administrative burden on entities to report, if they were to experience a material privacy breach. With regard to paragraph (b) above, HIF believes that these notification requirements are reasonable.

Implementation Timeline

HIF does not anticipate any issues with the implementation of CPS 234 and believes that, in line with the potentially material impact of information security incidents, the implementation timeline proposed by APRA, being 1 July 2019, is reasonable.

HIF thanks APRA for the opportunity to provide comment on the proposed requirements outlined in the Consultation Package.

Yours sincerely

Belinda Goosen
Chief Risk Officer

CC: Board
Audit and Risk Committee
Risk Management Committee