aamri

Association of Australian
Medical Research Institutes

CONSULTATION

STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES

20 August 2021

Contact:

Dr Peter Thomas
Executive Director
Association of Australian
Medical Research Institutes

[redacted]

Strengthening Australia’s cyber security regulations and incentives

1 About AAMRI

The Association of Australian Medical Research Institutes (AAMRI) is the peak body for medical research institutes across Australia. Our 49 member organisations work on a broad spectrum of human health issues such as preventive health, chronic disease, mental health, immunology and Indigenous health. Their research ranges from fundamental biomedical discovery through to clinical research and the translation of research findings from bench to bedside.

AAMRI’s members and their 19,000 staff and research students undertake over one-third of all government funded medical research. Their combined revenue exceeds $1.65 billion per annum, and they received over $622 million in competitive grant funding in 2016. With over 900 active clinical trials and over 100 new patents awarded per year, our members have a firm focus on improving health outcomes and delivering great commercial returns for the nation.

AAMRI welcomes the opportunity to provide comment on how businesses can be incentivised to invest and increase capabilities in cyber security. Having consulted with our members, the below comments on the highlighted issues are provided from a medical research institute (MRI) point-of-view.

2 Consultation feedback

2.1 Governance standards for large businesses

In the absence of clear Australian standards for assessing cyber security risk and maturity, MRIs utilised and adopted parts from different frameworks for example, the Australian Cyber Security Centre (ACSC) Essential Eight[1], National Institute of Standards and Technology (NIST) Framework (United States)[2]. Essential Eight was deemed to be very useful but the voluntary nature of the framework meant that uptake varied. More definitive guidance from the government around cyber security risks and maturity assessment to allow better benchmarking of progress would be beneficial.

MRIs currently report on their cyber security activities via different ways, including to the Board or via their risk, audit and governance committee. In general, senior executives i.e. Board members, CEOs, COOs etc. within MRIs understood the importance of cyber security. It is our view that education and awareness raising initiatives, such as case studies on breaches and failures, should be targeted towards the general workforce, who are less aware of these risks and considerations. Increasing awareness, Board level direction, and integrating cyber security considerations into corporate best practice and legal compliance would allow better financing and investment support and strengthen governance around cyber security risks.

2.2 Minimum standards for personal information

MRIs are covered under the Privacy Act, with their obligations around patient data and health information captured under various state legislations as well as sector-specific guidelines, including

[1] https://www.cyber.gov.au/acsc/view-all-content/essential-eight
[2] https://www.nist.gov/cyberframework

those from the National Health and Medical Research Council[3]. The inclusion of a cyber security code under the Privacy Act as well as the use of mitigation strategies covered under Essential Eight as technical controls would be effective. There should be flexibility around which levels and targets each MRI should aim for and comply with. Organisations should be allowed to assess their maturity levels and set targets based on the types of research activity that are undertaken within each MRI and within each project. For example, clinical trials involving patient data will have different requirements to discovery research that does not involve any human samples. The existing obligations under the Privacy Act and penalties for non-compliance could also be strengthened, for example to be more aligned with the European Union General Data Protection Regulation (GDPR)[4] or the California Consumer Privacy Act (CCPA)[5].

2.3 Mandatory product standard and labelling for smart devices

While MRIs do not generally make smart devices, the increase in Digital and e-Health applications mean the integrity of smart devices is crucial to allow sufficient protection of users and their health information. Having a mandatory product standard and labelling would be beneficial. Adopting internationally recognised standards for smart devices, similar to ISO standards for medical devices, increases transparency and will enable MRIs to appropriately choose the devices they use and develop applications for.

2.4 Responsible disclosure policies

As above, MRIs generally do not develop publicly available software or provide services online and therefore responsible disclosure policies are likely less relevant to the sector. The MRI sector's cyber security focus is largely targeted towards regular testing of cyber security capabilities and benchmarking against an agreed upon maturity framework. However, for MRIs that do develop software either for public use, or involving sensitive data, vulnerability assessments and reporting will be critical.

Additional clarification around responsible disclosure and further guidance on how responsible disclosure policies work will be helpful. From a consumer or user viewpoint, when selecting for services or businesses, it is likely that cyber security track records will already be available online. From a developer and service provider viewpoint allowing the reporting of near misses anonymously, rather than via public disclosures, may encourage more entities to voluntarily report threats. These threats could be disclosed either directly to the ACSC, or to other relevant regulators, without fear of negative impacts to their business or reputation. We are keen to better understand how the implementation of responsible disclosure policies will complement these measures to strengthen cyber security.

2.5 Voluntary health check for small businesses

Setting a minimum cyber security standard based on an agreed upon framework would be beneficial, for example, the Essential Eight. One of the key challenges faced by MRIs, which are not-for-profit charities with limited budgets, is the lack of funding available to enhance cyber security. Mandating, or at least strongly recommending, targets based on sector requirement and risk profiles would encourage investment by organisations to strengthen their cyber security. However, if this happens additional government funding needs to be provided to the MRI sector to meet their responsibilities in relation to protecting government funded medical research.

[3] https://www.oaic.gov.au/privacy/the-privacy-act/health-and-medical-research/

[4] https://gdpr-info.eu/

[5] https://oag.ca.gov/privacy/ccpa

2.6 Clear legal remedies for consumers

Consumer protection within the Privacy Act may be strengthened by aligning with the GDPR or CCPA, but the implementation costs of doing this need to be adequately supported. MRIs may contract third parties to progress activities that involve sensitive information, for example, the running of clinical trials or reaching out to donors. It is currently unclear whether the contracting party (MRIs) or the third party will be liable for data breaches, particularly if the contracting party have done all required due diligence prior to contracting the third party. Further guidance on this would be appreciated.