MSIA
MEDICAL SOFTWARE
INDUSTRY ASSOCIATION

MSIA Critical Infrastructure Security Submission

Department of Home Affairs

16/09/20

MSIA CEO | Emma Hossack

[redacted] | [redacted]

Medical Software Industry Association

PO Box 576, Crows Nest NSW 1585, Australia

P: 02 9431 8649

Executive Summary

The Medical Software Industry Association Ltd (MSIA) represents the interests of health software companies which power better outcomes for all Australians. Our members include large international corporations operating in Australia as well as small start up companies. MSIA members software is used by private, public and not-for-profit providers. It includes systems used in hospital specialist, aged care, indigenous, disabilities, allied, research, primary care and preventative care settings. Virtually all health information in Australia is collected, communicated and managed by our members software. The record for security and safety over the last 40 years is a source of great pride for our industry. We applaud the Department's initiative to hardening Australia's critical infrastructure. However in the likely event that the proposed legislation includes the health sector, it must be cognisant of the byzantine complexity of our industry and its place in providing critical services efficiently for all Australians.

The proposed enhancements to *Security and Critical Infrastructure Act 2018 (the Act)* include 3 elements:

- A positive security obligation for critical infrastructure entities supported by sector-specific requirements;
- Enhanced cyber security obligations for those entities most important to the nation, &
- Government assistance to entities in response to significant cyberattacks on Australian systems.

Our submission responds to all three elements which have application to our industry. These require a nuanced approach which is cognisant of existing and emerging frameworks and legislation. Our industry is impacted by numerous jurisdictional laws and Commonwealth legislation including the *My Health Records Act (2012)*, the *Health Identifiers Act (2010),* the *Health Insurance Act (1973)*, the *Privacy Act* (1988) and the *Private Health Insurance Act* (2007). All of these are predicated on compliance with strict security requirements, such as obtaining conformance for connection to critical infrastructure such as the MBS and PBS.

In addition, there are emerging obligations such as the ANAO recent audit into the implementation of *My Health Record* which necessitates implementation of a series of security measures which are to be enforced by the *Australian Digital Health Agency*. Other prevailing frameworks include the *National Health Information Strategy* by the *Australian Commission for Safety and Quality in Healthcare*, the sectoral Rules and Guidelines from peak bodies including the *Royal College of General Practitioners (RACGP) Computer and Information Security Standards* as well as emerging guidelines from the *ACCC* for *Digital Platforms Inquiry.* The *Therapeutic Goods Administration* also provides additional regulation which is currently being reviewed, to which the MSIA has provided guidance and considerations which is germane to this consultation.

The health software industry is heavily regulated by this complex web of laws, policies and guidelines. This framework has served Australia well and should be carefully considered in the context of the proposed changes. This is because excessive or inconsistent regulatory change will increase the burden on Australians responsible for managing health care for themselves and others as well as having direct and unnecessary cost burden on industry and its clients, the providers of all health care in Australia.

The enormous benefits of digital health through virtual care initiatives like ePrescribing and telehealth have never been so apparent as in 2020 with bushfires and COVID-19 highlighting the need for more flexible service delivery. The fiscal environment demands that we improve care delivery efficiently. Our industry is the powerhouse for innovation and productivity in Australia's health system which needs support and stimulation rather than more regulation. The proposed changes must be made in close consultation with our membership and we look forward to the engagement for a safer more resilient health system in Australia.

The MSIA is pleased the Department recognises that a 'one size fits all" approach is not appropriate and looks forward to a partnership with the Department to develop a balanced principles- based approach to proportionate changes the security of critical health infrastructure.

Yours Sincerely

Emma Hossack

CEO

MSIA 16 September 2020

	Call for views	MSIA Response
1	Do the sectors above[1] capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?	Apparently.
2	Do you think current definition of Critical Infrastructure is still fit for purpose?	Inclusion of health reflects the legislative intention. Harmonisation with other health legislation and frameworks will be critical.
3	Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?	The MSIA has recently provided an issues paper to the TGA which refers to the over-arching controls by health professionals in the use of tools like software. This factor needs to be considered as a major safeguard in the event of security threats.
4	What are the common threats you routinely prepare for and those you have faced/experienced as a business?	Our member companies and their clients may use on-premises licensed software of platform/software as a service. All are impacted by the usual malicious Malware routinely addressed by the Cyber Security Centre as well as hardware and internet failures. Specifics can be provided.
5	How should criticality be assessed to ensure the most important entities are covered by the framework?	Assessments should evolve with the Threat Risk Assessments which will be key to this area. Each vertical in health has different levels of security depending on sensitivity and the workforce capability. E.g. Aged care records are managed very differently to youth mental health records.
6	Which entities would you expect to be owners and operators of systems of national significance? **Additional Question:** Should owners and operators be subject to the same requirements?	Systems of National significance would presumably include systems such as My Health Record which is operated by a Government Agency which is appropriate. It is understood that Health Assets such as those operated by our members software would not be considered Systems of National Significance (SONS). Consultation would be required urgently if this was not the case.

COLLABORATION TO SUPPORT UPLIFT

	Call for views	Response
7	How do you think a revised Trusted Information Sharing Network for Critical Infrastructure (**TISN**) and Critical	

[1] • Banking and finance • Communications • Data and the Cloud • Defence industry • Education, research and innovation • Energy • Food and grocery • Health • Space • Transport • Water

	Call for views	Response
	Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	*More information required in respect of how this could function with existing information flows and privacy settings in health.*
8	What might this new TISN model look like, and what entities should be included?	*As above*
9	How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus? **Additional Question:** What should be Government responsibility and what should be the responsibility of industry in this relationship?	*As above*

Initiative 1 – Positive Security Obligation

	Call for views	Response
10	Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	Yes.
11	Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	The draft legislation is not available – it is not possible to answer without this fundamental information.
12	Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?	The MSIA has visibility of some sectoral security postures with which it members service. Whilst some have sophisticated threat responses, others are still operating in a paper world. All have differing levels of capability and would need significant time and resources to meet the principles.
13	What costs would organisations take on to meet these new obligations?	Insufficient information to know what the specific requirements would be. Irrespective of the legislative principles (which are not provided). It should be noted that all parties involved in health transactions from the consumers through to software providers could however be impacted.
14	Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?	The Australian Privacy Principles (APPs) mandate the security (APP 11) and accessibility of information for sensitive information like health information (APP 12). The other legislation referred to in the Executive Summary also impose obligations. These are likely to be supplemented by the requirement of the AIHW National Health Information Strategy and the Modernisation programme being implemented by Services Australia. Also the ADHA response and implementation of the ANAO requirements following the audit of the MHR implementation. There are also security and related reporting obligations under the My Health Records Act for providers and software vendors that connect to that system.

	Call for views	Response
		The costs of satisfying all of these requirements is significant. The specifics of business continuity may not be sufficiently covered by the APP 12.
15	Would the proposed regulatory model avoid duplication with existing oversight requirements?	Without details of draft legislation it is not possible to respond fully. However a principles - based approach is consistent with the APPs and should be complimentary to the further security requirements of the other legislation referred to in the Executive Summary.
16	The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?	Harmonisation of the Commonwealth and Jurisdictional requirements with those of the various health entities and professional bodies would be invaluable. Guidance should be evolving and : • Clear and consistent; • Able to be practically implemented given workforce constraints; • Based on a known threat/ risk assessment basis;
17	Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?	Apart from the Agencies mentioned, Services Australia, ADHA, the OAIC and ACCC (which can act as the FDA do in the USA in respect of security & privacy and misrepresentation)there is no actual regulator of security for health. Having a cross sector regulator with an overarching role for all industries which could be calibrated according to risk would be the most efficient model and avoid confusion in a very complex sector.
18	What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?	Regular industry engagement and briefings.
19	How can Government better support critical infrastructure in managing their security risks?	• Consistent education sessions for all verticals in health including providers, consumers and industry with a targeted approach to each. All parties need to work cohesively on this as a single weak link can be fatal as the Shergold Report demonstrated, • Some sectors like aged care will need financial assistance and education to become digital and cyber resilient, & • Playbooks.
20	In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a	The use of existing registries in health may be more appropriate e.g. AHPRA Services Australia modernisation programme will be leveraging off work done with the Digital Transformation Agency, ADHA and others on credentialing like PRODA etc.

	Call for views	Response
	similar model be useful in the sectors you are familiar with?	Not all industries have the same requirements – e.g. Blue Card is not essential for Residential Aged Care Workers but critical in educational facilities. Even the ISM is not broadly accepted as being the optimal solution for health. This requires further consultation.
21	Do you have any other comments you would like to make regarding the PSO?	It is an area where the cost and burden could outweigh the benefit and have serious negative unintended consequences.

Initiative 2 – Enhanced Cyber Security Obligations

- The MSIA understand the no health assets, systems or entities are being classified as SONS. Consequently this section is not addressed.

- Advise if this is not the case and further consultation will be essential.

Advise #	"Call for views"	Response
22	Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?	N/A
23	What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing? **Additional Question:** How can the Government effectively share aggregated threat information? Is there an existing process that works well?	N/A
24	What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?	N/A
25	What methods should be involved to identify vulnerabilities at the perimeter of critical networks?	N/A
26	What are the barriers to owners and operators acting on information alerts from Government?	N/A
27	What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?	N/A
28	What safeguards or assurances would you expect to see for information provided to Government?	N/A

Initiative 3 – Cyber Assistance for Entities

All or part of the MSIA membership could be subject to Government Assistance measures as a supplier and operator of **Critical Infrastructure Assets** in health- defined as *assets, systems or networks involved in the provision of health care, production of medical supplies and medical research*.

As with any deployment of emergency powers, the usual issues of privacy, contractual obligation and excessive force de majeure are key concerns. A proportionate response is both expected and reflected by the proposed framework. Further details would assist in building trust for such measures.

The type of exceptions in section 95 of the Privacy Act use public health and serious harm as over-riding consideration. Whilst the greater public good is logical, there must be absolute **transparency of process to engender the kind of trust** the public has given to the Commonwealth Government in reaction to many COVID-19 responses.

Appropriate reparation needs to be embedded where financial loss is sustained as a result of Government intervention.

	Call for views	Response
29	In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	Similar to COVID-19 response, the Health Minister, Prime Minister and Chief Medical Officer should all have a role in declaration of emergency, together with State and Jurisdictional Premiers where relevant
30	Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?	As above
31	Who should oversee the Government's use of these powers?	Under the Constitution, there may be a role for the Governor General, Judicial Review or Government Ombudsman
32	If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?	It will be determined by the facts
33	What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	Crown Immunity
34	What safeguards and oversight measures would you expect to ensure the necessary level of accountability for this type of powers?	Full Judicial Review
35	What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?	Fear doubt and uncertainty remain the biggest risks to industry. Clear, constant and consistent messaging and communication is key.
36	Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?	Following consultation in respect of the specific legislative amendments to the Act, the MSIA can provide a comprehensive response to the proposed safeguards and unintended consequences and their mitigation.