MSIA
MEDICAL SOFTWARE INDUSTRY ASSOCIATION

Cyber Security Regulation
Submissions on the discussion paper

Date: 27 August 2021

Contact: Emma Hossack | [redacted] | [redacted]
[redacted]


1stGroup
ACSSHEALTH
Adventist HealthCare
ALCIDION
Allscripts
5 Faces
MEDILINK
Clinicalabs
ADG
AutoMed Systems
Ben Connell
Best Health Solutions
Best Practice
binary
caps Clinic
CARDIHAB
careMonitor
Cerner
CHAMONIX
citadel health
CIVICA
CLINIC CLOUD
clintel
COMPACT SYSTEMS AUSTRALIA
comrad
DIRECT CONTROL medical
Corum Health
COVIU
Cubiko
Dedalus
ScriptPro
Doctors on Demand
D.R.A COMPUTING
eHealthWise
episoft
eRx script exchange
eucalyptus
evrima
EXTENSIA
foxo
FRED
IQRS
INTEGRATED QUALITY RISK & SAFETY
Genie Solutions
guildlink
MedicalDirector
Health Intersections
Health Metrics
HealthEngine
Health Link
RxOne
Specialist Complete
HELLO SUNDAY MORNING
HLLS
HotDoc
humanetix
cutting edge
Hyland
SOX
SURGICAL ORDER
InfoMedix
Infoxchange
iCIMS
integrated software solutions
InterSystems
Creative data technology
Intrahealth
Healthcare
jarvishealth
JAYEX
kestral
leecare
lysn
MANAGE MY HEALTH
McCauley Software
medAdvisor
Dox
Medical Records
medical objects
medi map
Medipass
MediRecords
MediSecure
MEDITECH EXPANSE
medmate
MEDrefer
medtech
OUTCOME HEALTH
MetaOptima
MIMS 100% pure knowledge
MODEUS
monkey
Mountaintop Systems
NET HEALTH
NEXT PRACTICE
PPMP PRACTICE MANAGEMENT SOFTWARE
NPS MEDICINEWISE
Ocean HEALTH SYSTEMS
OEXA
ORACLE
ORIDASHI
Pacific Knowledge Systems
palcare
pencs
PHARMHOS
POS WORKS
GO nourish
consentic intelligent consent
praxhub
Precedence Health Care
Presagen AI enhanced healthcare
pro medicus
Provider Assist
Qscan
ResApp HEALTH
Roche
rose mary
Scrypt.
SIEMENS Healthineers
simple retail
SmarTek
SmartHealth SOLUTIONS
smartsoft
SONIC HEALTHCARE
Stat
ONE PASSPORT
SURGICAL PARTNERS
minfos
HEALTH
THE CLINICIAN
hello home doctor SERVICE
tiikr
TOUCH STONE
AutumnCare
varian A Siemens Healthineers Company
VMORE practice people
VISUAL OUTCOMES
webstercare
WeKo
xestro
Z SOFTWARE
ZEDMED

Executive Summary

The Medical Software Industry Association (**MSIA**) applauds the Government for its initiative in releasing this discussion paper. The quality of cyber security is critical in most industries, but arguably of most importance to health, as recognised by the *Critical Infrastructure Bill.*

MSIA members represent over 95% of providers of all the health software used throughout Australia in primary, secondary and tertiary care. This includes Aged Care, Disabilities, Community Care, Hospital care, Allied Care, General Practice, Specialists, Telehealth, Secure Messaging, Indigenous care, Chronic Disease management and financial and administrative services relating to all of these areas. As such, the MSIA members collect process and manage virtually all the health and well-being data of Australians. This is the most sensitive information which is extremely attractive to bad actors.

The MSIA has made submissions in respect of the *Digital Economy Strategy, Review of the Privacy Act 1988 issues paper* and the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*. Our members are committed to a resilient digital economy which we realise depends on clear, fit for purpose, affordable and enforceable cyber security rules.

Our members enabled the transformation of medication through COVID-19 to rapidly developed capability to enable the upload of immunisations to the Australian Immunisation Register, facilitate consumer bookings and enable remote care with the introduction of an entirely seamless paperless virtual prescribing enabling end to end consumer care via telehealth consultations through to dispense of medications. The success of these, and many other innovations depend on the trust of consumers and health providers. This in turn requires a strong security framework.

For over 30 years our members have collected and managed the most sensitive and valuable information in Australia.

One of the major impediments which our members and their clients, the health professionals face, is the lack of clarity about how data can be managed safely, securely, usefully for the health and well-being of all Australians. The patchwork of Commonwealth and State legislation, policies and protocols deployed by public and private entities leads to uncertainty. The result is to default to not sharing data in cases where it would be extremely valuable to do so, or to share in good faith but without appropriate guidance on the guard rails this can be dangerous[1]. Contrary to the interests of individual autonomy and missed opportunities for innovation, research and efficiency. It can also result in failure to observe minimal standards required and inappropriate action by unauthorised third parties whose concern to promote security and privacy can have negative unintended consequences.[2]

[1] Information to Share or not to share – The Information Governance Review https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf. The Caldicott review commissioned in 1997 as a result of the avoidable death of a little girl through lack of information sharing led to a transformation in the way health providers and others share information in the UK – a series of reports including this one provide guidance and confidence to people to act humanely and appropriately.

[2] Some outfits promote what they see as shortcomings on websites to embarrass or coerce organisations which may in fact have appropriate frameworks for their context but lack of a Government imprimatur makes this difficult to manage.

The MSIA welcomes this opportunity to input into this seminal discussion paper which could for improve the life of all Australians.

The MSIA responds to the discussion papers three pillars namely: Clear Expectations, Transparency and Consumer Rights. We will not comment on Devices and Labels.

Clear Expectations

MSIA members want a clear co-designed framework which can be efficiently implemented. We welcome the opportunity to be involved in this process.

The MSIA represents an ecosystem of providers across the spectrum from large multinationals to small start-ups. Many of these systems interconnect, but the future demands of our health system call for more interconnectivity to improve the quality of care, consumer UX and efficiency. Consequently, to avoid issues with supply chain and silos where, for example, a smaller system and larger system connect, there needs to be a baseline to avoid companies cutting connection with or refusing to connect to systems which have a lower level of security.

A voluntary code which is co-designed and reflects international standards would be ideal, but there needs to be careful consideration of ecosystems and divergent resources within those ecosystems to avoid the unintended consequence of more silos.

Mandated standards are not desirable at a time of extreme pressure for our industry which is responding to an array of Government requirements in response to COVID-19 and the Services Australia modernisation. Furthermore, unless there is both a well-resourced regulator and extensive education for end users, added security requirements will be meaningless.
A voluntary code could evolve over time to a mandated code following consumer education and appropriate resourcing to ensure that there is a level playing field.

Transparency and Disclosure

The MSIA supports the creation of an environment consumers, researchers and the public generally are encouraged to report security vulnerabilities directly with organisations, vendors and service providers.

The current position is unclear and leads to unauthorised and/or untrained actors to “blowing the whistle” over alleged vulnerabilities by publicly naming and shaming. We agree that where legitimate direct approaches are impractical or unsuccessful, security vulnerabilities should be

reported to the ACSC which can direct unverified vulnerabilities to other agencies where appropriate.[3] Disclosure programmes appear to be a useful approach.[4]

A health check for small businesses is a good idea and a health check trust mark is supported by the MSIA. We understand this could be effectively implemented by building on existing and evolving self-assessment tools[5]. The information asymmetries, where sellers are in a better position to understand the cyber security of their digital products and services than buyers, specifically affects our industry. By helping organisations and individuals to better understand the risks this asymmetry could be addressed. This would and assist industry, reduce the supply chain risk and improve the overall security posture for Australia.

Protection of Consumer Rights

The MSIA supports additional hardening of the Australian Consumer Law to encourage all organisations to prevent cyber security incidents in addition to existing protections against misleading and deceptive conduct.

We agree that a direct right of action could give individuals greater control over their personal information and provide an additional incentive for entities covered by the Privacy Act to comply with their obligations under the Act.

Summary

A clear cyber security code of practice, co-designed by industry, Government and consumers is critical for our digital economy. It is foundational to the trust which underlies decisions to participate – or not – in the digital environment.

The MSIA looks forward to the response to the discussion paper and active engagement in the crucial next steps which must be taken in the context of the other reviews on the digital economy, Privacy Act and Critical Infrastructure.

Emma Hossack

CEO
MSIA

[3] https://www.cyber.gov.au/sites/default/files/2020-08/18.%20ISM%20-%20Guidelines%20for%20Software%20Development%20%28August%202020%29.pdf

[4] https://developers.google.com/android/play-protect/ starting-a-vdp or the European Union's Google Practice Guide on Vulnerability Disclosure at https://www.enisa.europa.eu/publications/ vulnerability-disclosure.

[5] https://business.gov.au/news/is-your-business-cyber-secure