Consumers Health Forum of Australia

SUBMISSION

CONSULTATION: MEDICAL DEVICE CYBER SECURITY

February 2019

Consumers Health Forum of Australia 2019 C*onsultation: Medical Device Cyber Security.* Canberra, Australia

P: 02 6273 5444
E: info@chf.org.au

twitter.com/CHFofAustralia
facebook.com/CHFofAustralia

Office Address
7B/17 Napier Close,
Deakin ACT 2600

Postal Address
PO Box 73
Deakin West ACT 2600

Consumers Health Forum of Australia is funded by the Australian Government as the peak healthcare consumer organisation under the Health Peak and Advisory Bodies Programme

CONTENTS

Contents

Background

Consumers Health Forum of Australia (CHF) is the national peak body representing the interests of Australian healthcare consumers and those with an interest in health care consumer affairs. CHF works to achieve safe, quality, timely healthcare for all Australians, supported by accessible health information and systems.

CHF appreciates the opportunity to provide a comment to the Therapeutic Goods Administration (TGA) consultation on Medical Device Cyber Security.

At the heart of CHF's policy agenda is patient-centred care. Our responses to the TGA's consultation has been formed with a patient-centred approach in mind.

CHF notes that this consultation's scope is limited to the regulatory guidance in line with existing regulatory requirements, and not changes to those regulatory requirements. However, as other consultations are currently open to change regulations for Software as a Medical Device (SaMD) it would be remiss for CHF to not include some forward-looking advice on out of scope but related matters.

Issues and recommendations

A central tenet of our healthcare system is the need for consumers to be able to give informed consent to treatment. In the context of medical devices, a central challenge to ensuring that consent is informed is in the effective communication and understanding of risk, when neither the clinician or the consumer is an expert in cybersecurity. Therefore, the requirements for manufacturers of devices, regulators and policy makers to provide clear, high quality and usable information to clinicians and consumers about cybersecurity risks and how to mitigate them should meet a higher bar than in areas where it is reasonable to expect one party has a high level of expertise.

Part 1 - Guidance for industry

The CHF largely supports the proposed guidance for manufacturers and sponsors. We believe that clearly articulating the way in which addressing medical device cybersecurity needs is required by the existing regulations will draw those needs to the forefront of manufacturer consideration.

A guiding principle in consumer-friendly software development is to incorporate privacy and security 'by design'. The CHF strongly urges that, when considering cybersecurity, medical devices incorporate not only security by design but also consumer privacy by design and consumer understanding by design. We support the inclusion of secure-by-design and quality-by-design concepts in the draft, and can see a case for going further.

Communicating to consumers about the way a device has been fundamentally designed to protect their privacy and security should help ameliorate concerns many have that by communicating risk to consumers they may be scared away from appropriate and effective treatment. **Therefore, CHF recommends that the industry guidance expand the Pre-market section of Part 1 in the draft to include mention of privacy by design, and to include the suggestion that this is also the stage at which to consider how the manufacturer will communicate to consumers and clinicians about the risks of the device.**

Appendix 6 of the draft contains examples of known medical device cyber security vulnerabilities. We presume that the list in Appendix 6 of the proposed guidance is not an exhaustive list. As such **we recommend that the guidance include reference to other resources that manufacturers, sponsors and consumers can refer**, to ensure that they are aware of all potential cybersecurity threats that need to be considered.

Part 2 – Guidance for consumers

The CHF believes that the current guidance to consumers is too general and needs to be supplemented by medical device specific cybersecurity guidance. It would be nigh impossible for the guidance given to consumers to cover all the possible cybersecurity risks and how to mitigate them, so instead **we recommend that the guidance for consumers focus on helping consumers understand the right questions to ask** when considering these issues. CHF also recommends that workshops be done with consumers and industry to arrive at the most pertinent and helpful questions. Those core questions would also provide a clear guideline for manufacturers to meet when they are developing their consumer facing information. For example, consumers could consider;

- Was this device made to be secure by design?
- What default settings are there to protect me?
- When and how does this device connect to the internet?
- What data is collected by the device, where does it go, and who has access to it?
- What risk is there to me if that data gets into the wrong hands, and how likely is that to happen?
- How can I tell if my device has been hacked or compromised? Who do I talk to if I think it might have been?

This question-based approach may be particularly useful for improving Appendix 7 – Consumer Factsheet. Advice about precautions to take needs to be specific to the device where possible, for example so that consumers whose devices only connect to the internet in controlled settings like a doctor's office are not concerned by the advice given to consumers whose devices are always connected through a smartphone.

Further information that could be provided in this guidance also includes common actions that may increase or decrease a device's cybersecurity status, what adverse events relating to cyber security look like, what actions should be taken if they feel their device is compromised, how to report breaches of device cybersecurity or a device not being as cybersecure as expected, and who to contact for help. Further work with consumers should be done to improve the relevance and helpfulness of this guidance over time.

CHF believes that additional guidance should be provided to healthcare providers to allow for them to properly communicate with and inform consumers who are considering devices with cybersecurity risks. eIFUs for devices must include this information. CHF notes that production of a consumer eIFU for medical devices could assist both consumers and industry in reducing the risk profile of devices, and **recommends that the guidance to manufacturers include the suggestion to make something like a consumer eIFU available to consumers, and the guidance to consumers include information on how to find them** if they exist.

CHF recommends that the TGA or another area of the Department of Health take an active role in communicating the cybersecurity considerations of medical devices not only to industry but also to consumers, leveraging groups such as educators, GP clinic, websites such as healthDirect and so on to ensure that consumers become aware of these risks when considering medical devices.

Digital health and cybersecurity is a fast moving area, and as such **CHF recommends that the guidance for consumers be presented as a web page as well as PDF, and that it undergoes frequent and regular revision and improvement**. We would be happy to discuss with the TGA further ways that consumers could help keep the guidance current, applicable, and helpful.

Cybersecurity and other TGA reforms

Given the both the high number of software and firmware programs that can be used in devices and the rapid rate of updates and other changes; the CHF recommend that the TGA adopt a process of 'whitelisting' device software and firmware that are more likely to be secure, rather than blacklisting ones that are known to not be cybersecure.

Additionally the TGA should take an active role in post-market monitoring and communications to ensure that if devices being used by consumers are compromised, particularly high risk devices and implantable devices, prompt notification to device recipients of identified risks and patches is possible.

CHF urges that as many consumers will be unaware of the technical details of cybersecurity, default settings and system be set such that risk is minimised. This includes things such as not having default administrator access password, having updateable firmware, ensuring device recipients can be contacted in the event of identified breaches and patches etc.