Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia

Timothy Webb, Sumer Dayal *

Intellectual Property & Technology, Clayton Utz Lawyers, Sydney, NSW, Australia

Keywords:
Cybersecurity
Medical devices
Food and Drug Administration
Therapeutic Goods Administration

ABSTRACT

Cybersecurity in medical devices has become a pressing issue in modern times. Technological progress has simultaneously benefited health care and created new risks. Through examining regulatory guidance, this article establishes that stakeholders have a shared responsibility to address cybersecurity threats that can affect such devices. Manufacturers and health care providers should consider identification, detection and prevention steps at the pre-market and post-market stages. End users and medical practitioners should practice good cyber hygiene to mitigate cybersecurity risks. Collectively, increased collaboration across all stakeholders is fundamental to ensure effective protection.

1. Introduction

Healthcare, as with most sectors, is becoming increasingly digitised in modern times. In an age where smartphones and wearable devices have the capacity to store and transfer mass volumes of data on our physical activity, calorie intake and sleeping patterns, it is only natural for the healthcare industry to take advantage of wireless technology to improve patient care. However, increased benefits come with increased risks. Devices that employ wireless technologies could be vulnerable to hacking and expose a patient's data, or the devices themselves, to malicious forces. Studies have begun to recognise this issue and often place healthcare in their top industries at risk of cybersecurity threats such as distributed denial of service (DDoS) attacks and theft of personal data.[1]

Understanding how to mitigate cybersecurity risks is therefore crucial for all health care stakeholders (including patients and other end users, health care facilities, independent health care providers and manufacturers of medical devices). This article considers the guidance that has been provided by regulatory authorities (including the Australian Therapeutic Goods Administration (**TGA**) and the United States Food & Drug Administration (**FDA**)) and other sources to inform stakeholders of cybersecurity risks and ensure that each one of them is contributing to the "shared responsibility" of preventing medical devices from becoming compromised.

2. The state of the technology – wireless networks and medical devices

Medical devices that use wireless technology are widespread, ranging from external pumps and monitors to implantable

* *Corresponding author.* Clayton Utz, Level 15, 1 Bligh Street, Sydney, NSW 2000, Australia.
E-mail address: twebb@claytonutz.com; sdayal@claytonutz.com (S. Dayal). https://www.claytonutz.com/.

[1] See e.g., IBM, *IBM X-Force Threat Intelligence Index 2017: The year of the mega breach* (March 2017) and IBM, *Security trends in the healthcare industry* (2015) at 12–13; see generally Avi Rubin, 'All your devices can be hacked', *TEDxMidAtlantic* (October 2011) available at: https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked/transcript?language=en#t-259833.

http://dx.doi.org/10.1016/j.clsr.2017.05.004
0267-3649/

Please cite this article in press as: Timothy Webb, Sumer Dayal, Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.004

visual aids, pacemakers and neurostimulators. Similarly, health care entrepreneurs have begun investing in apps and devices that store and transmit high levels of patient data for improved healthcare services. Projected targets for growth include apps for monitoring heart conditions, detecting concussions, providing video consultation services and "telemedicine" services for collating medical records and corresponding with doctors online. The TGA is conscious of this development – medical software is considered to be a 'medical device' if it fulfils the criteria under Australian therapeutic goods legislation.[2] In the U.S.A., the FDA approved 36 connected health apps and devices in 2016 alone.[3]

The TGA and FDA have actively considered the issue of cybersecurity in medical devices.[4] For example, the FDA has raised the possibility of unauthorised users gaining remote access to infusion pump systems, while both regulatory bodies have turned their attention to potential vulnerabilities in implantable cardiac devices and defibrillators.[5] Last year, the TGA provided a safety update identifying infusion, insulin and implantable drug pumps, implantable cardiac defibrillators, neural stimulators, heart monitors and infant/foetal monitors as vulnerable devices, though no cybersecurity attacks had been reported in Australia. The spectrum of potentially exposed devices is therefore broad.[6]

The risks will come as no surprise to software developers. An oft-cited estimate is that people writing source code make between 10 to 50 errors in every 1000 lines of code. Careful checking can reduce the error rate, but error free software is deemed impossible. As modern programming can contain millions of lines of code, the potential for thousands of bugs to exist in software offers the possibility of exploitation.[7] Recent events such as the 'Wannacry' cyberattack demonstrate the potential for software vulnerability exploitation to become a large-scale epidemic.[8]

However, as the FDA has noted, the same features that expose a medical device to cybersecurity threats also improve health care and increase the ability of health care providers to treat patients.[9] For example, systems that wirelessly connect to and receive the data stored on an implantable cardiac device and send it to a patient's medical practitioner(s) via a healthcare network demonstrably improve the practitioner's ability to provide patient care, but raise their own risks of intrusion.

The question then is one of balance – how do manufacturers and entrepreneurs use wireless technologies to enhance patient outcomes and simultaneously guard against the threats that such technologies expose?

3. "A shared responsibility"

The TGA and FDA recognise that the onus of mitigating and managing cybersecurity threats is shared across all healthcare stakeholders. From pre-market to end utilisation, each stakeholder has continuing obligations to maintain the barrier against cybersecurity threats.

3.1. *Manufacturers and health care providers*

Medical device manufacturers (and health care providers by extension) have a particular onus to mitigate, or take steps to mitigate, the risk of cybersecurity vulnerabilities and maintain effective safeguards throughout a product's lifecycle.

The FDA divides its advice into premarket and postmarket management. In the pre-market stage, manufacturers are encouraged to address cybersecurity vulnerabilities during the design and development of the medical device for ap-

[2] See TGA, 'Regulation of medical software and mobile medical 'apps'' (13 September 2013) available at: https://www.tga.gov.au/regulation-medical-software-and-mobile-medical-apps.

[3] See 'A digital revolution in health care is speeding up', *The Economist*, 2 March 2017 available at: http://www.economist.com/news/business/21717990-telemedicine-predictive-diagnostics-wearable-sensors-and-host-new-apps-will-transform-how?cid1=cust/ednew/n/bl/n/2017032n/owned/n/n/nwl/n/n/AP/9012562/n.

[4] See particularly, the FDA's webpage on medical device cybersecurity available at: https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm and the TGA's 'Medical Devices Safety Update', vol 4, number 2, March 2016 (29 February 2016) available at: https://www.tga.gov.au/publication-issue/medical-devices-safety-update-volume-4-number-2-march-2016.

[5] See FDA, 'Symbiq Infusion System by Hospira: FDA Safety Communication – Cybersecurity Vulnerabilities' (31 July 2015) available at: https://www.fda.gov/safety/medwatch/safetyinformation/safetyalertsforhumanmedicalproducts/ucm456832.htm; See FDA, 'Implantable Cardiac Devices and Merlin@home Transmitter by St. Jude Medical: FDA Safety Communication – Cybersecurity Vulnerabilities Identified' (9 January 2017) available at: https://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm535979.htm and St Jude Medical's response announcing cybersecurity updates at http://media.sjm.com/newsroom/news-releases/news-releases-details/2017/St-Jude-Medical-Announces-Cybersecurity-Updates/default.aspx; see J Medew, 'Thousands of pacemakers and defibrillators 'at risk of hacking'', *The Age*, 6 February 2017 available at: http://www.theage.com.au/victoria/thousands-of-pacemakers-and-defibrillators-at-risk-of-hacking-20170205-gu5w65.html.

[6] See 'Medical Devices Safety Update' above n 4.

[7] See 'Why everything is hackable: Computer security is broken from top to bottom', *The Economist*, 8 April 2017 available at: http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security.

[8] At the time of writing, it was reported that the ransomware had spread to 150 countries with approximately 200,000 victims. Affected institutions included the UK's National Health Service and hospitals that were unable to access patient data and experienced disruptions in emergency care services: see 'NHS cyberattack: GPs and hospitals hit by ransomware', *BBC News*, 13 May 2017 available at: http://www.bbc.com/news/health-39899646 and 'More than 150 countries affected by massive cyberattack, Europol says', *The Washington Post*, 14 May 2017 available at: https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?utm_term=.4fc1c233ffa9.

[9] FDA, 'Cybersecurity' (last updated 3 March 2017) available at: https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm; See also Federal Trade Commission, *Internet of Things: FTC Staff Report* (January 2015) at 7–8 available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Please cite this article in press as: Timothy Webb, Sumer Dayal, Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.004