US regulators react to cyber threats to medical devices

Cyber attacks against connected medical devices are a growing area of concern for regulators. Regulatory action in the US so far includes the Food and Drug Administration's ('FDA') 'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices' guidance, which *inter alia* addresses the key elements necessary for establishing a cyber security management system. Sonali P. Gunawardhana and Megan L. Brown of Wiley Rein LLP discuss the regulatory response so far in the US.

In the healthcare area, the amount of potentially accessible personal health data is vast and complex, and promises to grow as innovators create new health focused products, services and applications. In a recent study[1], 94% of healthcare institutions were reported to have been victims of cyber attacks.

Cyber security threats targeting computer connected medical devices are a growing area of concern for regulators. Medical devices can be vulnerable to security breaches that may impact the safety and effectiveness of the devices. This vulnerability increases as medical devices are becoming more connected through the internet to hospitals, insurance providers, and to other medical devices. An increase in cyber attacks on medical devices has been noted by the Department of Homeland Security ('DHS')[2]. Although these attacks have been primarily associated with disruption due to malicious programs and viruses and have not directly affected patient safety, policy makers see a threat that needs to be addressed[3]. In fact, the FDA has addressed this issue in various ways over the past year in order to try to mitigate the risk of cyber security threats to medical devices in the future.

On 13 June 2013, the FDA issued a Safety Communication, entitled 'Cybersecurity for Medical Devices and Hospital Networks,'[4] in which the FDA recommended that medical device manufacturers and healthcare facilities take steps to ensure that appropriate safeguards are adopted to reduce the risk of device failure due to a cyber attack. To further its efforts, the FDA on 26 August 2014 entered into a Memorandum of Understanding ('MOU') with the National Health Information Sharing and Analysis Center ('NH-ISAC'). NH-ISAC is a non-profit health sector led organisation that provides member organisations with actionable information on cyber security and coordinates incidence responses. The primary goals of this MOU are to foster stakeholder collaboration, create awareness about the National Institute of Standards and Technology's ('NIST') voluntary cyber security framework, and to encourage healthcare stakeholders to develop innovative strategies to access and mitigate cyber security vulnerabilities[5].

The FDA has also issued three guidance documents that put forth recommendations to medical device manufacturers on cyber security management as well as information that should be included in the device manufacturer's premarket submissions for review by the Agency. The final FDA guidance document entitled, 'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,' issued on 2 October 2014, addresses some key elements of establishing a cyber security management system[6]. The guidance states that, as a best practice, manufacturers should address cyber security concerns during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks. In addition, the FDA stated that manufacturers should establish design inputs for their device related to cyber security, and establish a cyber security vulnerability and management approach as part of the software validation and risk analysis that is required by 21 C.F.R.§ 820.30(g)[7]. The guidance goes on to state that the approach should appropriately address the following elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies; and
- Assessment of residual risk and risk acceptance criteria[8].

The Agency also recommends that medical device manufacturers consider their cyber security activities by reference to the framework established by NIST for Improving Critical Infrastructure Cybersecurity[9]. NIST convened private and public sector stakeholders to develop a voluntary cyber security framework for critical infrastructure entities. It is intended to be the centrepiece of a voluntary program run by the DHS and will guide various sector specific agencies to evaluate and improve the nation's cyber security posture. It is organised around five core functions - Identify, Protect, Detect, Respond, and Recover - and provides suggested uses and approaches for companies large and small to assess their abilities in each area. The ultimate goal is to help the private sector focus on cyber security with a common language and shared goals.

NIST is evaluating the private sector's understanding and use of the Framework, and industries are in the process of mapping existing best practices to it. For example, the FDA is collaborating with the NH-ISAC to 'adapt and operationalize the NIST Framework for Improving Critical Infrastructure Cybersecurity.'[10] Much remains to be done, however, and the private sector continues to emphasise that the NIST Framework is not a roadmap for regulatory expectations or standards. Nonetheless, in the absence of broad data and cyber security standards, the Framework is likely to be used as a starting point for regulatory activities, which could range from reporting and informational obligations to prescriptive regulation.

Endorsement by sector specific agencies could turn the voluntary Framework into a *de facto* standard or standard of care. The Federal Trade Commission ('FTC') has been expanding its authority over data security and is expected to be aggressive when it comes to consumer health information. As an example, the FTC sued the medical testing laboratory LabMD, Inc. alleging that 'the company failed to reasonably protect the security of consumers' personal data, including medical information.'[11] In that litigation, the parties have disputed whether NIST guidance and other standards are adequate to put private businesses on notice of regulatory expectations. The FTC and other agencies can be expected to leverage the NIST Framework in their expectations for the private sector.

Endorsement by sector specific agencies could turn the voluntary NIST Framework into a *de facto* standard or standard of care

Although the FDA's guidance documents are non-binding, they outline the FDA's views on manufacturers' responsibilities for remaining vigilant about identifying cyber security risks and hazards associated with their medical devices and hospital networks that could be caused by the introduction of malware into the medical equipment or unauthorised access to configuration settings. These guidance documents also explain the need for appropriate mitigation plans to address patient safety and assure proper device performance. The FDA believes that developing an effective set of cyber security controls should reduce the risk to patients by decreasing the likelihood that device functionality is compromised by inadequate cyber security.

Given the difficulty of addressing cyber security threats to all stakeholders involved, the FDA along with the DHS also held a public workshop this past October to bring together medical device manufacturers, healthcare providers, biomedical engineers, IT system administrators, professional and trade organisations, insurance providers as well as local, state and federal government representatives to discuss both the challenges that lie ahead as well as areas in which there is consensus on best practices to mitigate cyber security risks. Participants were asked to 'identify barriers to promoting medical device cybersecurity; discuss innovative strategies to address challenges that may jeopardize critical infrastructure; and enable proactive development of analytical tools, processes, and best practices by the stakeholder community in order to strengthen medical device cybersecurity.'[12]

Most stakeholders seem to grasp at least some of the perils of cyber security threats, and all that work in this area must understand that successfully mitigating them requires collaboration and communication. Given the uncertainties that exist on the adequacy of rapidly evolving threats and solutions, industry should watch and participate in FDA and related proceedings involving cyber security. Technical standards rapidly evolve, so continued collaboration and communication are essential to addressing and mitigating risks in the healthcare industry, including keeping medical devices free from cyber attacks.

Sonali P. Gunawardhana Of Counsel
Megan L. Brown Partner
Wiley Rein LLP, Washington DC
sgunawardhana@wileyrein.com
mbrown@wileyrein.com

[1] Filkins B. SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon. Norse February 2014.
[2] Finkle, J. 'U.S. government probes medical devices for possible cyber flaws,' Reuters, 22 October 2014.
[3] Ibid.
[4] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm
[5] http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm
[6] 'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff,' 2 October 2014.
[7] 21 CFR Part 820 - Quality Systems Regulations: 21 CFR 820.30 Subpart C - Design Controls of the Quality System Regulation.
[8] 'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff,' 2 October 2014 at p. 6.
[9] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
[10] http://www.nhisac.org/blog/fda-and-nh-isac-collaboration/
[11] http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter
[12] http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm