Sonali P. Gunawardhana Of Counsel
sgunawardhana@wileyrein.com
Wiley Rein LLP, Washington DC

The US FDA's Final Guidance on Postmarket Management of Cybersecurity in Medical Devices: the important changes to note

Sonali P. Gunawardhana, Of Counsel at Wiley Rein LLP, provides detailed analysis of the US Food and Drug Administration's ('FDA') final guidance on 'Postmarket Management of Cybersecurity in Medical Devices' and the changes adopted by the FDA in response to stakeholder responses.

The FDA recently finalised a guidance document entitled 'Postmarket Management of Cybersecurity in Medical Devices.' The draft guidance was issued in early 2016 and received 54 comments during the comment period. Many of these comments were posted by individuals, medical device companies and various associations representing a wide array of interests. There were several changes in the finalised guidance and many seem to represent the FDA's willingness to address commenters' concerns. The key principles of this document were outlined by the FDA during a 12 January 2017 webinar, as follows:

- Use a risk based framework to ensure risks to public health are addressed in a continual and timely fashion;
- Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and postmarket authorities;
- Foster a collaborative and coordinated approach to information sharing and risk assessment;
- Align with Presidential EOs and the NIST framework; and
- Incentivise the 'right' behaviour[1].

Key changes

'Essential Clinical Performance'

Many comments included a request that the FDA eliminate the term 'essential clinical performance' from the guidance (because the term appeared to be newly used by the agency), or, alternatively, revise the definition of the term to be consistent with IEC 60601-1 (which requires compliance with ISO14971). Although the term 'essential clinical importance' incorporated the concept of harm, it also included ambiguous concepts such as 'acceptable' and 'unacceptable' clinical risk. The Advanced Medical Technology Association, better known as AdvaMed, stated that, "while 'essential clinical performance' may be easily defined in a simple case, such as a medical device with one intended use and minimal connectivity, it does not translate well for complex situations and environments[2]."

It appears that in response to the comments received from various filers the FDA has changed nearly all references to 'essential clinical performance' to 'patient harm.' This change in terminology appears to shift the way in which the FDA plans to evaluate cyber security risk and align the terminology with current FDA recognised standards. The FDA's current thinking on cyber security risk seems to now be more focused along the lines of the potential harm to the patient. The guidance now includes the following language which exemplifies this shift: 'this guidance recommends how to assess whether a risk of patient harm is sufficiently controlled or uncontrolled. This assessment is based on an evaluation of the likelihood of exploit, the impact of exploitation on the device's safety and essential performance, and the severity of patient harm if exploited[3].' One of the possible reasons for this shift is that the term 'patient harm' is simpler for manufacturers to apply across the board as that is how manufacturers currently comply with reporting requirements under 21 C.F.R. Part 806. The FDA included a definition of the term 'patient harm' given the term was not used in the draft guidance. In order to provide greater clarity in regards to current FDA thinking the agency defined patient harm 'as physical injury or damage to the health of patients,

image: Andy Roberts / OJO Images / Getty Images

It appears that in response to the comments received from various filers the FDA has changed nearly all references to 'essential clinical performance' to 'patient harm.'

continued

including death. Risks posed by the device may result in patient harm[4].'

Information Sharing Analysis Organisations

The FDA also received many comments regarding more information as to the FDA's vision of the benefits associated with industry's participation in an Information Sharing Analysis Organization ('ISAO'). Many agreed with the FDA that the sharing of threat information is likely to benefit patient safety but were concerned with the FDA's recommendation that the ISAO is the only type of organisation that could possibly provide comparable benefits.

Additional information was requested as to how the FDA intends to participate in the ISAO, which ISAO is acceptable in terms of participation by a medical device manufacturer, and the role of the ISAO and its responsibilities. With respect to ISAOs the FDA clarified in a newly added section the definition of active participation by providing specific criteria and stated again in the final guidance document that 'the Agency considers voluntary participation in an ISAO as a critical component of a medical device manufacturer's comprehensive proactive approach to management of postmarket cybersecurity threats and vulnerabilities and a significant step towards assuring the ongoing safety and effectiveness of marketed medical devices[5].' During the webinar, some participants asked questions regarding what safeguards would be put into place to safeguard against hackers. The FDA responded by stating that the information would be considered protected data and that the ISAO infrastructure is rigorous enough to safeguard the information and that information would be shared in a particular manner, stripping it of attributions.

Other changes

Some other areas of change include that software changes made to strengthen cyber security are not typically subject to Part 806 recall reporting requirements so long as they meet certain criteria. One criterion that was outlined in the draft guidance document required implementing device changes and compensating controls within 30 days of becoming aware of a cyber security vulnerability. The FDA modified this requirement to state that it should be completed 'as soon as possible but no later than 30 days of learning of the vulnerability[6].' The 30 day remediation timeframe outlined in the draft guidance has been expanded to include a 60 day tier in the final guidance.

Areas of additional clarity/expansion

There were other notable areas where the final guidance provided additional clarity, including:

- By expanding the scope of the guidance to expressly include mobile medical applications ('MMAs').
- By adding that upgrades to increase confidentiality protection are also not generally subject to Part 806 reporting requirements.
- Establishing that routine cyber security updates and patches will not generally require premarket review, however, these routine updates and patches could change other functionality of the device and therefore must be evaluated to determine whether premarket review is required.
- By adding a new section entitled 'Examples of Vulnerabilities Associated with Controlled Risks and their Management.' In this section the FDA provides four examples of instances in which a device manufacturer becomes aware of cyber security vulnerability after the device has been commercialised.

Takeaway message

This final guidance imposes some significant new requirements on manufacturers of devices with potential cyber security vulnerabilities. It is clear that device manufacturers believe that patient safety is a number one priority and that a successful cyber security program needs to include action by more than simply the manufacturer. As the FDA has taken the total product life cycle approach to cyber security, hence device manufacturers with legacy products will have to consider cyber security vulnerability for a wide range of products including software that is not specifically part of the medical device and for devices that are not inter-connected but have software that can make it vulnerable. The one area that remains constant from the draft guidance that the FDA did not expand on was how it plans to enforce the recommendations set out in the guidance. During the webinar, FDA officials did state that the timing for compliance is immediate but to assume there will be a learning curve in effect. Only when future events of cyber security issues of vulnerability are identified and addressed will we see how well the final guidance has provided a framework for navigating an ever changing area of technology.

1. FDA/CDRH Webinar Presentation Slide Deck, 'Postmarket Management of Cybersecurity in Medical Devices- Final Guidance,' p. 9.
2. AdvaMed and MITA Comments Re: Docket No FDA-2015-D-5105 Postmarket Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff. Availability p. 2.
3. Postmarket Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff. 28 December 2016 p. 10 Definitions, Section F. Patient Harm.
4. Postmarket Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff. 28 December 2016 p. 10 Definitions, Section F. Patient Harm.
5. Postmarket Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff. 28 December 2016 p. 8 Section II. Background.
6. Postmarket Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff. 28 December 2016 p.22 Section VII. Part B. Remediating and Reporting Cybersecurity Vulnerabilities/Uncontrolled Risk to Safety and Essential Performance.