HealthManagement
Promoting Management and Leadership

Tiered FDA medical device security guidance concerns industry

The U.S. Food and Drug Administration (FDA) recently released its draft guidance on managing cybersecurity in medical device premarket submissions. In the draft, a **two-tiered system for identifying cyber risk** is proposed, with higher risk devices falling into Tier 1 while other devices would be of “Standard Cybersecurity Risk” or Tier 2.

You might also like: Medical device partnerships for better healthcare solutions

However, leading companies such as GE Healthcare and industry groups have voiced **concerns over the tiered approach**, saying this will result in confusion and potential discrepancies. They want the tiered system eliminated or amended. Industry group AdvaMed, for instance, said that the planned two-tier framework is "unnecessary given its superficial similarity" to FDA’s risk classification scheme for medical devices.

The group is urging the FDA to remove the two-tiered approach "in favour of a single risk-based approach that addresses the Agency’s cybersecurity expectations based on the exploitability of a device vulnerability and the severity of patient harm (if exploited), as outlined in the Agency’s postmarket cybersecurity guidance.”

The Medical Imaging and Technology Alliance (MITA) has called the tiered system unclear and seeks more **clarity with regard to issue of patient harm.** “How will the FDA distinguish between a medical device for which a cybersecurity incident could directly result in patient harm to multiple patients, and one that does not? What does the phrase ‘harm to multiple patients’ mean in practice?”

GE Healthcare also found the two tiers “somewhat confusing and vague,” but suggested explicit criteria for an additional Tier 3 for “Low Cybersecurity Risk.” Such a third tier, the company said, could help prevent the inclusion of non-electronic medical devices such as tongue depressors into Tier 2. "We do not believe there is value in stating that a tongue depressor or blood pressure cuff has ‘Standard Cybersecurity Risk’ in a premarket submission,” the company pointed out.

Becton, Dickinson and Company (BD), for its part, called for the creation of a tier-less system to “promote implementation of equal security measures for all types of devices. It would also eliminate potential discrepancies and **disagreements that can arise from classifications.**”

Should the FDA decide to retain the current tiers, this is what BD recommends: “Tier 1 devices should also include a risk-based rationale. Risk-based rationale for Tier 1 devices should describe intended use scenarios, technological limitations, or risk-benefit trade-offs that preclude the implementation of specific control(s).”

Source: Regulatory Affairs Professionals Society (RAPS)
Image credit: Pixabay

Published on : Tue, 26 Mar 2019