BARNES & THORNBURG LLP

ALERTS

FDA Issues Draft To Update Prior Final Guidance On Premarket Cybersecurity For Medical Devices

October 23, 2018 | Indianapolis | Washington, D.C.

The FDA recently issued a draft guidance document titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." The draft guidance states that, when finalized, it will replace the final guidance issued in October 2014, with the same name. According to the FDA, "the rapidly evolving landscape, and the increased understanding of the threats and their potential mitigations, necessitates an updated approach."

The draft guidance introduces two categories of medical devices for cybersecurity purposes:

Tier 1 "Higher Cybersecurity Risk"

A medical device is a Tier 1 device if the following criteria are met:

1) The device is capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, or to a network, or to the internet; and

2) A cybersecurity incident affecting the device could directly result in harm to multiple patients.

Examples of Tier 1 devices include, but are not limited to, implantable cardioverter defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps, and the supporting connected systems that interact with these devices such as home monitors and those with command and control functionality such as programmers.

Tier 2 "Standard Cybersecurity Risk"

A medical device for which the criteria for a Tier 1 device are not met is considered a Tier 2 device.

Not surprisingly, the guidance notes the different tiers have different regulatory requirements and cautions that the tiers do not necessarily track the statutory device classifications (Classes I, II, and III).

The major sections of the draft guidance address three topics: design, labeling, and documentation.

Designing a Trustworthy Device: Application of NIST Cybersecurity Framework

A "trustworthy device" is defined as "a medical device containing hardware, software, and/or programmable logic that: (1) is reasonably secure from cybersecurity intrusion and misuse; (2) provides a reasonable level of availability, reliability, and correct operation; (3) is reasonably suited to performing its intended functions; and (4) adheres to generally accepted security procedures."

RELATED PEOPLE

Lynn C. Tyler, M.S.
Partner
Indianapolis

P 317-231-7392
F 317-231-7433
lynn.tyler@btlaw.com

RELATED PRACTICE AREAS

Drug and Medical Device

The draft guidance includes detailed design recommendations for (1) preventing unauthorized use of the device, (2) ensuring trusted content, (3) maintaining confidentiality of date, and (4) detecting, responding to, and recovering from cybersecurity threats. It recommends that premarket submissions for Tier 1 devices include "documentation demonstrating how the device design and risk assessment incorporate the cybersecurity design controls described" in the guidance. For Tier 2 devices with standard cybersecurity risk, the FDA recommends that premarket submissions include documentation that (1) demonstrates they have incorporated each of the specific design features and cybersecurity design controls described in the guidance, or (2) provides a risk-based rationale for why those cybersecurity design controls are not appropriate.

Labeling Recommendations

Per the draft guidance, the FDA recommends that when drafting labeling for inclusion in a premarket submission, a manufacturer should consider all applicable labeling requirements and how informing users through labeling may be an effective way to manage cybersecurity risks. The draft guidance includes several specific recommendations for details to include in labeling to communicate relevant security information to end-users.

Cybersecurity Documentation

In general, the FDA recommends that manufacturers include documentation of the design features, risk management, and labeling – in accordance with the draft guidance – to demonstrate a risk-based approach that incorporates features and a level of cybersecurity appropriate for the device. To this end, the draft guidance includes several specific recommendations for design documentation and risk-management documentation.

Interested parties may submit written comments on or before March 18, 2019, at regulations.gov.

As always, the FDA's guidance documents do not establish legally enforceable responsibilities, but rather describe the FDA's current thinking on a topic.

For more information, please contact the Barnes & Thornburg attorney with whom you work or Lynn Tyler, chair of the firm's Food, Drug & Device group, at 317-231-7392 or lynn.tyler@btlaw.com.