BARNES & THORNBURG LLP

ALERTS

Food, Drug And Device Law Alert - FDA Issues Draft Guidance On Cybersecurity For Medical Devices

January 19, 2016 | Atlanta | Chicago | Columbus | Dallas | Delaware | Elkhart | Fort Wayne | Grand Rapids | Indianapolis | Los Angeles | Minneapolis | South Bend

The Food and Drug Administration (FDA) recently issued a draft guidance, "Postmarket Management of Cybersecurity in Medical Devices," addressing cybersecurity in medical devices. The draft guidance applies to "(1) medical devices that contain software (including firmware) or programmable logic, and (2) software that is a medical device." According to the FDA, medical devices are increasingly connected to computer networks to facilitate patient care and, as a result, may be vulnerable to cybersecurity threats. The draft guidance "emphasizes that manufacturers should monitor, identify and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices."

The 25-page draft is detailed and not readily susceptible to being summarized. Unfortunately, it will also require careful study by the manufacturers of devices that fall within its scope as described above. Some of the highlights are discussed below.

Essential Clinical Performance

One of the key concepts in the draft guidance is "essential clinical performance," defined as "performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer." If essential clinical performance is compromised, there may be harm to the patient or intervention may be required to prevent harm to the patient.

Managing Medical Device Cybersecurity Risk

The draft guidance states that throughout the medical device lifecycle a medical device firm should establish, document, and maintain an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls, as part of their risk management process consistent with 21 CFR part 820. The process should include risk analysis, risk evaluation, risk control, and incorporation of production and post-production information. The draft guidance includes an appendix identifying the elements which should be included as part of the manufacturer's cybersecurity risk management program. According to the guidance, firms should have a defined process to conduct systematically a risk evaluation and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk. FDA recommends that firms define and document their process for objectively assessing the cybersecurity risk for their device(s).

RELATED PEOPLE

Lynn C. Tyler, M.S.
Partner
Indianapolis

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

RELATED PRACTICE AREAS

Food, Drug and Device Law

The draft guidance recommends that the firm's defined process focus on assessing the risk to the device's essential clinical performance by considering:

1. The exploitability of the cybersecurity vulnerability, and
2. the severity of the health impact to patients if the vulnerability were to be exploited.

The analysis should also incorporate consideration of compensating controls and risk mitigations.

After discussing the assessment of these two factors, the draft guidance proposes a matrix to assess the risk to essential clinical performance for the identified cybersecurity vulnerabilities. The draft guidance states the figure below can be used to assess the risk to the device's essential clinical performance from a cybersecurity vulnerability as controlled or uncontrolled:

Mitigation of Cybersecurity Risk

In all cases, the FDA recommends firms take the following steps to mitigate cybersecurity risk:

- Proactively practice good cyber hygiene, and reduce cybersecurity risks even when residual risk is acceptable;
- Remediate cybersecurity vulnerabilities to reduce the risk of compromise to essential clinical performance to an acceptable level;\
- Conduct appropriate software validation under 21 CFR 820.30(g) to assure that any implemented remediation effectively mitigates the target vulnerability without unintentionally creating exposure to other risks;
- Properly document the methods and controls used in the design, manufacture, packaging, labeling, storage, installation and servicing of all finished devices as required by 21 CFR part 820
- Identify and implement compensating controls, such as a work-around or temporary fix, to adequately mitigate the cybersecurity vulnerability risk, especially when an "official fix" may not be feasible or immediately practicable. In addition, manufacturers should consider the level of knowledge and expertise needed to properly implement the recommended fix;

- Provide users with relevant information on recommended work-arounds, temporary fixes and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use.

When the cybersecurity risk for a medical device is evaluated as "controlled" or acceptable, the draft guidance advises:

- Changes to a device that are made solely to strengthen cybersecurity are typically considered device enhancements, which may include cybersecurity routine updates and patches, and are generally not required to be reported, under 21 CFR 806.10;
- For premarket approval (PMA) devices with periodic reporting requirements under 21 CFR 814.84, newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of cybersecurity routine updates and patches should be reported to FDA in a periodic (annual) report.

When the cybersecurity risk for a medical device is evaluated as "uncontrolled" or unacceptable, the draft guidance recommends the following actions:

- Manufacturers should remediate the vulnerabilities to reduce the risk of compromise to essential clinical performance to an acceptable level;
- When an official fix may not be feasible or immediately practicable, manufacturers should identify and implement risk mitigations and compensating controls, such as a work-around or temporary fix, to adequately mitigate the risk;
- Manufacturers should report these vulnerabilities to the FDA according to 21 CFR part 806, unless reported under 21 CFR parts 803 or 1004. However, the FDA does not intend to enforce reporting requirements under 21 CFR part 806 if all of the following circumstances are met:
    - There are no known serious adverse events or deaths associated with the vulnerability,
    - Within 30 days of learning of the vulnerability, the manufacturer identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users, and
    - The manufacturer is a participating member of an Information Sharing Analysis Organization (ISAO), such as the National Health Information Sharing & Analysis Center (NH-ISAC);
- Remediation of devices with annual reporting requirements (e.g., Class III devices) should be included in the annual report;
- The manufacturer should evaluate the device changes to assess the need to submit a premarket submission (e.g., PMA supplement, 510(k), etc.) to the FDA;

- The customer base and user community should be provided with relevant information on recommended work-arounds, temporary fixes and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use;

- For PMA devices with periodic reporting requirements under 21 CFR 814.84, information concerning cybersecurity vulnerabilities, and the device changes and compensating controls implemented in response to this information should be reported to FDA in a periodic (annual) report.

A copy of the draft guidance can be found here.

For more information, please contact the Barnes & Thornburg LLP attorney with whom you work or one of the following attorneys in the firm's Food, Drug & Device Group: Lynn Tyler at (317) 231-7392 or lynn.tyler@btlaw.com; or Alicia Raines at (317) 231-7398 or alicia.raines@btlaw.com.

Visit us online at www.btlaw.com/food-drug-and-device-law-practices.