BARNES & THORNBURG LLP

ALERTS

Food, Drug And Device Law Alert - FDA Issues Final Guidance On Postmarket Management Of Cybersecurity In Medical Devices

January 4, 2017 | 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 final guidance titled "Postmarket Management of Cybersecurity in Medical Devices." The guidance applies to "(1) medical devices that contain software (including firmware) or programmable logic, and (2) software that is a medical device, including mobile medical applications." In an expansion from the draft version, the final guidance also applies to devices that are part of an interoperable system and "legacy" devices, i.e., devices already on the market or in use.

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 guidance "emphasizes that manufacturers should monitor, identify and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices."

The 30-page guidance is detailed and not readily susceptible to being summarized. Like the draft version, the final guidance 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.

Postmarket Considerations

According to the guidance, it is essential that manufacturers implement comprehensive cybersecurity risk management programs and documentation consistent with the Quality System Regulation (21 CFR part 820), including but not limited to complaint handling (21 CFR 820.198), quality audit (21 CFR 820.22), corrective and preventive action (21 CFR 820.100), software validation and risk analysis (21 CFR 820.30(g)) and servicing (21 CFR 820.200).

The FDA states that cybersecurity risk management programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm. Critical components of such a program include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk
- Maintaining robust software lifecycle processes that include mechanisms for:

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

    - monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle
    - design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to off-the-shelf software
- Understanding, assessing and detecting presence and impact of a vulnerability
- Establishing and communicating processes for vulnerability intake and handling
- Using threat modeling to define clearly how to maintain safety and essential performance of a device by developing mitigations that protect, respond, and recover from the cybersecurity risk
- Adopting a coordinated vulnerability disclosure policy and practice
- Deploying mitigations that address cybersecurity risk early and prior to exploitation

In this connection, the guidance notes the FDA has recognized ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes and ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure which may be a useful resource for manufacturers.

The guidance "strongly recommend[s]" that manufacturers participate in an information sharing and analysis organization (ISAO) that shares vulnerabilities and threats that impact medical devices.

Managing Medical Device Cybersecurity Risk

The 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 its 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 guidance includes an appendix identifying the elements that should be included as part of the manufacturer's cybersecurity risk management program. According to the FDA, firms should define and document their process for objectively assessing the cybersecurity risk for their device(s).

The 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.

The 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:

Reporting and Remedying Cybersecurity Risk

The FDA recommends firms take the following steps to mitigate cybersecurity risk:

- Adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the initial vulnerability report to the vulnerability submitter
- 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
- 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
- Recognize that some changes made to strengthen device security might also significantly affect other device functionality (e.g., use of a different operating system) and assess the scope of change to determine if additional premarket or postmarket regulatory actions are appropriate

When the cybersecurity risk for a medical device is evaluated as "controlled" or acceptable, the 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
- Even when risks are controlled, manufacturers may wish to deploy an additional control(s) as part of a "defense-in-depth" strategy. Typically, these changes would be considered a cybersecurity routine update or patch, a type of device enhancement
- Device changes made solely to address a vulnerability that, if exploited, could lead to compromise of PHI, would typically be considered a cybersecurity routine update or patch
- 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 guidance recommends the following actions:

- Manufacturers should remediate the vulnerabilities to reduce the risk of compromise to 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 must 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 for specific vulnerabilities with uncontrolled risk under certain circumstances set forth in guidance
- 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
- 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 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; Beth Davis at (404) 264-4025 or beth.davis@btlaw.com; or Alicia Raines Barrs at (317) 231-7398 or alicia.rainesbarrs@btlaw.com.

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

Visit us online at www.btlaw.com and follow us on Twitter @BTLawNews.