Bloomberg BNA

Privacy Law Watch™

Medical Devices

Views on Cybersecurity Risk Management in Postmarket Medical Devices From Ballard Spahr Co-Head of Privacy and Data Security Philip N. Yannella

The Food and Drug Administration Jan. 22 released draft guidance on cybersecurity risk management of postmarket medical devices—a medical industry term for devices that have been released in the market after research and clinical trials—recommending that manufacturers monitor and track cybersecurity information sources and alert users within a certain time frame depending on the severity of the cybersecurity threat.

Bloomberg BNA Privacy & Data Security News Senior Legal Editor Daniel R. Stoller posed a series of questions to Philip N. Yannella, partner at Ballard Spahr LLP and co-practice leader of the firm's Privacy and Data Security Group, on how the cybersecurity risk management guidelines affect the postmarket medical device industry.

 ISSN 0000-0000

BLOOMBERG BNA: What is your take on the Food & Drug Administration's (FDA) guidance on the cybersecurity risk management of postmarket medical devices that says there is no notification requirement for ''controlled risks'' and a notification requirement for ''uncontrolled risks''?

PHILIP N. YANNELLA: It is an intelligent way to proceed. The FDA needs to be concerned about threats that affect the safety of the device and the welfare of the patients. The FDA is using the standard ''Essential Clinical Performance'' meaning anything that affects the ability of the device to achieve the clinical outcomes to make or keep the patient healthy. Compromise of the essential clinical performance would produce a hazardous situation that would result in harm to the patient and would require intervention to prevent that harm to the patient.

The risk matrix and analysis the FDA suggests allows a manufacturer to balance the exploitivity and severity impact to patient health. The manufacturer can use the matrix to assess the risk to essential clinical performance. Routine updates and upgrades do not require reporting.

In essence, the reporting requirement is consistent with Executive Order 1636, Improving Critical Infrastructure Cybersecurity. It assesses threat levels and then responds accordingly.

For example, if ports on the device are open and can be accessed to tamper with the performance of the device, but requires physical access to the device which is implanted in the patient, the risk is mitigated by the limited physical access. Taking action to close the device ports and alerting the patient and doctor to the threat is sufficient to mitigate or ''control'' the risk and need not be reported.

However, if the device can be accessed remotely and tampered with and the tampering may affect the essential clinical performance of the device (i.e. over inject insulin in an insulin pump), then that would require reporting to the FDA. It is a very reasonable approach, which ensures the safety and welfare of the patient without overburdening the resources of the FDA.

The scope of risk is real. The same enhancements and technology that allow cardiologists, for example, to adjust a patient's pacemaker for optimal effect, also allow hackers, if uncontrolled, to breach security for that pacemaker and effect the essential clinical performance.

BLOOMBERG BNA: How would your firm's Data Security Emergency Response Team assist a client whose post-market medical device caused ''serious adverse effects or death,'' thus triggering mandatory notification requirements?

YANNELLA: We would immediately respond, help the client assess the threat level and alert patients and physicians as well as the FDA. We would guide the client in a strategy that would alleviate future actions deleterious to the patients using the device and ensure the client in keeping with all FDA regulations.

We are experts at the assessment matrix and guide the client to the proper procedures to restore patient safety, notify the FDA and alert the patients and physicians to mitigate the risk to patient, manufacturer and the public health.

BLOOMBERG BNA: What is the scope of cybersecurity risks for postmarket medical devices and what future cybersecurity risks can you envision in the medical device market?

YANNELLA: The scope of risk is real. The same enhancements and technology that allow cardiologists, for example, to adjust a patient's pacemaker for optimal effect, also allow hackers, if uncontrolled, to breach security for that pacemaker and effect the essential clinical performance.

As devices and technology progress the threats will also progress. More sophisticated equipment means increased, new and greater threats. However, we do believe, properly employed, the new threat matrix suggested by the guidance will severely limit threat potential and create a greater environment of safety.

BLOOMBERG BNA: What are the cost and benefits for companies joining a cooperative such as a Information Sharing and Analysis Organization (ISAO)?

YANNELLA: ISAO participation reduces reporting requirements to the FDA considerably. From a legal standpoint, I would go so far as to say it reduces liability also, in the fact that it shows the manufacturers commitment to safety and negates any ill intent on the manufacturers part.

Of course every situation varies and to protect a manufacturer's trade secrets and intellectual property, while sharing information to preserve device and patient safety, consulting with a law firm that has the expertise necessary to handle that complex area would be critical to success.

  PRA ISSN 0000-0000

ISAO participation reduces reporting requirements to the FDA considerably. From a legal standpoint, I would go so far as to say it reduces liability also, in the fact that it shows the manufacturers commitment to safety and negates any ill intent on the manufacturers part.

BLOOMBERG BNA: How will the implementation of the recommended risk management programs by medical device companies impact their economic outlook?

YANNELLA: If done properly, using ISAO data sharing and the NIST Framework for improving critical infrastructure, the costs to a manufacturer should be reasonable. The increased security should increase the physician and patient confidence in the safety of medical devices and encourage greater use.

As with all additional Quality Systems requirements, if integrated appropriately into the design and post market monitoring of the device, the economic impact should be no more than compliance with various sections of 21 CFR 820 for QSR, complaint handling, quality audit, corrective and preventive action, software validation and risk analysis and servicing and monitoring. Companies who have good Quality Assurance systems will have little additional cost or trouble implementing the new guidance recommendations.

Yannella would like to thank Neil DiSpirito, of counsel Ballard Spahr, for his assistance.