Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Medical Device Cybersecurity: Preparing For The Worst

By **Sonali Gunawardhana and Chris Harvey** (April 23, 2018, 3:18 PM EDT)

Sonali Gunawardhana

Chris Harvey

Medical device manufacturers create new products to help patients, never imagining they might be used to do harm. But the fast rise of malicious hacking of devices in the home and in health care facilities has introduced new risks to both patients and health care providers.

U.S. hospitals use approximately 10-15 connected devices per hospital bed. And consumers are increasingly using connected devices from home to monitor their own health without giving much thought to security vulnerabilities like public Wi-Fi. Data exposed through hacking could be used for fraud, identity theft, supply chain disruption, intellectual property theft and more. Hacking is disruptive and dangerous to patient care, and may put manufacturers in legal jeopardy.

Medical device manufacturers understand cybersecurity vulnerabilities pose a threat, but are not sure where to begin. The U.S. Food and Drug Administration has issued guidance to help them address and respond to threats and attacks. But given the potential pitfalls of a medical device cybersecurity breach, attorneys need to ensure their clients are prepared for a security-related product recall in the event a breach does occur. They should also take the lead in counseling clients through the concrete steps that may prevent hacking, but that are often overlooked.

Preparing for the Inevitable

Perhaps the most important strategic step for a medical device manufacturer is to prepare for the worst. Even when preventative steps are taken, a cybersecurity vulnerability may surface that requires a product recall. In some cases, these may be fixed with an over-the-air update. But many patches still require a visit to a medical provider.

In other cases, such measures may be deemed insufficient, necessitating a traditional recall. In representing medical device manufacturers, attorneys should strongly advise clients to develop, test and maintain a robust recall plan — not just an outline of a plan.

Manufacturers should consider their internal teams and the level of expertise they bring to the table. Too often, an employee charged with managing recalls moves on from the company and the role is not assigned to someone else. That leaves a significant void when another recall occurs. In other cases,

those assigned to manage product recalls aren't familiar with the expectations of regulators.

Another factor to consider is consignee data. In the event of a device recall, hospitals and other medical offices will typically need to be notified directly. If facilities have changed locations, that data may be obsolete. It's important to proactively cross-check contact information across systems, or employ a recall partner to update the information.

In instances where the recall reaches the consumer level, companies must be prepared for the response. In general, the higher the hazard level, the greater the attention. The media and the public are acutely aware of hazards that could cause serious harm. That means having a scalable contact center staffed with agents who have medical and/or sensitivity training.

A patch may resolve a cybersecurity recall, but in cases where that isn't an option, products must be returned, processed and stored. In those instances, manufacturers must consider data collection, tracking capabilities and documentation for regulatory reporting.

Additional factors may add even more complexity. For example, if recalled products contain lithium-ion batteries, they may fall under specialized transportation and disposal regulations — regardless of whether the issue involves the batteries themselves.

It's also important to address cybersecurity threats at the design and development phase of the device, and even into the post-market stage, particularly with highly connected devices. Manufacturers should invest in a strong IT infrastructure with layered security and firewalls to deter hacking across all layers of the device.

Recall Fatigue

An additional obstacle for manufacturers to overcome is "recall fatigue." Product recalls occur with such exhaustive regularity across all industries that they are becoming lost on many consumers, creating safety and brand damage risks for medical device manufacturers.

Think about the current stream of direct mail, emails and news stories about recalls and it's no wonder consumers are experiencing recall fatigue. Medical device and other product recalls have reached an all-time high, with more than 3,400 last year. It can be challenging to connect with consumers whose antennae are muted to take action.

Manufacturers must work to ensure recall fatigue is minimized, especially when potentially life-threatening products such as medical devices are in the mix. By refining communications approaches to reach consumers where they like to consume information, such as on mobile devices, manufacturers have a better chance of compliance.

Sharing Is Caring

Manufacturers should also consider joining an information sharing analysis organization. Attorneys may have to be more persuasive with this step since clients are often reluctant to share information with competitors. But leaders increasingly recognize that industry-wide threats impact them all, and collaboration is the best recourse.

Medical device companies that operate globally should also be aware of international regulations. A

recent report issued by the Royal Academy of Engineering in the U.K. noted that "[i]n the EU, there is a regulatory framework for medical devices that aims to ensure that devices are safe for patients, but it has not fully considered the possible impacts of poor cybersecurity on patient safety or privacy." The report goes on to list several recommendations, including the formulation of a task force between the FDA and the U.K.'s Medicines and Healthcare products Regulatory Agency "to consider how the existing legislative frameworks can be strengthened."

Another good step is to use white hat hackers to find vulnerabilities that might otherwise go unnoticed. This technique is especially helpful for smaller companies that often lack IT resources. Unlike their malicious counterparts, these hackers exist solely to expose threats so they can be corrected early, and they are passionate about their profession.

In the end, connected medical devices are improving the lives and survival rates of patients. But in the race to innovate with technology, serious security concerns can arise when hackers choose to exploit holes in those innovations. With so many factors to consider, many manufacturers feel lost. Experts in recall prevention and preparation, in partnership with good legal counsel, can provide the roadmap necessary to protect the public and mitigate legal and regulatory risk.

Sonali P. Gunawardhana is of counsel at Shook Hardy & Bacon LLP in Washington, D.C. Chris Harvey is director of recall solutions at Stericycle Expert Solutions.