LAW360

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

How To Minimize Risk When Launching Smart Medical Devices

By **Anne Li, John Fuson and Gage Javier** (September 13, 2022, 6:01 PM EDT)

Anne Li

As the smart medical device industry expands at dizzying speed, more companies than ever before are entering the market.

Prior to launching a smart medical device there are several critical aspects to consider regarding device approval and company and patient protection.

This article explores protecting intellectual property, getting U.S. Food and Drug Administration approval and ensuring cybersecurity of a device's data.

Intellectual Property

John Fuson

When navigating IP issues for smart devices, companies can no longer simply patent incremental improvements to create a thicket, try to keep trade secrets or simply work to protect them.

Protecting smart devices requires an omnibus approach that involves building fences around your device and developing a nimble strategy that blocks competitors and includes utility patents and trade secrets, as well as design patents, copyright, trademarks and trade dress.

These decisions involve flexibility, understanding and factoring in the ever-changing case law interpretations, and the rapidity that drives software and device configuration innovation.

Gage Javier

For standard medical devices, all the usual strategies around patent and trade secret apply. But, for the software interface, data output, and what or how patients are monitored, traditional utility patent protection may not be the best option — especially because a lot of this innovation is not patentable even though it is valuable.

Also, trade secrets may not work to protect all the algorithms because the medical practitioners need to understand the data they are receiving and what it means.

Here are some practical tips:

Standardize the output into a distinctive format.

Courts have held that trade dress protection applies to the format of electronic medical records. Standardizing output for trade dress protection can be a valuable tool, especially with a first-in-type smart device.

Using design patent protection provides a head start on enforceable exclusive rights while medical practitioners adopt that format as the standard. This will slow competitor's growth because there will be an adoption curve in the medical field for the new output.

Trade-secret part of the software.

All the data collected can be used to generate a score for each patient using a trade secret algorithm. This will help patients understand the output more easily: For example, a red-yellow-green model or a numeric scale of 1-10. This may be reverse engineered and will need to be validated, but could provide a powerful tool to delay competitors.

Patent what you think will last.

This can be tricky in the shifting case law interpretations of patentability, but if there are certain aspects that are core to the smart device — electronic components, configured in a certain way, etc. — getting patent protection for those aspects will be crucial in keeping competitors off the market.

Patent on the fast track.

For key innovations that competitors may copy, an ounce of prevention is worth a pound of cure. Spend the extra money and file patents on Track 1 — the fast track.

For a few extra thousand dollars in fees up front, creating patent protection quickly is critical. And, when doing so, file claims in four groups, including narrow claims to protect your core technology, broader claims and claims directed at deterring your competitors — a broad set and a narrow set.

The idea is to get at least a few allowed quickly and file divisionals for others. This will help create a patent thicket as fast as possible in this dynamic field.

Use design patents, copyright and trademark to protect product designs, including physical device and visual displays and reports.

Many companies rely on product and house trademarks, but in this field, maximizing design protection will allow the holy grail of IP protection — it can last forever.

So, as new devices come out, updates occur, etc., having a strategy to protect them with consistent source identification that may be rooted in early or basic protection from design patent or copyright will last always.

It applies to so much more than just names, so it can be used much more broadly than it is currently, especially for the physical configuration of, and output from, smart devices.

Protecting smart medical devices requires the same flexibility, ingenuity, and creativity that developing

them does.

FDA Regulatory Considerations

The FDA's premarket review process is built around comparisons to previously marketed devices as the basis for marketing clearance.

This poses a challenge for manufacturers of new smart devices offering novel technologies and solutions to medical care: Obvious or appropriate predicate devices to reference in a submission may not exist.

A de novo classification request, which provides a pathway for the FDA to classify novel medical devices, is often the solution in such cases, but the de novo pathway leads to a longer, more complicated and less certain review process than a standard Section 510(k) submission.

Before taking that path, manufacturers may be well-served by engaging with the FDA to explore all possible options for bringing new beneficial devices to market. A Section 513(g) request for information or a presubmission meeting with the agency may help illuminate the most expeditious pathway to FDA clearance for a new smart device.

513(g) Request for Information

Section 513(g) of the Federal Food, Drug and Cosmetic Act directs the FDA to respond within 60 days to any written request with a written statement of the classification of the proposed device and the regulatory requirements applicable to it.

As the FDA has explained, the response will include the agency's assessment of the generic category and class that the proposed device appears to fall within, which marketing application, if any, is appropriate for the device, and which regulatory requirements are applicable to the category of the device and whether additional regulatory requirements may apply to the specific case.[1]

For novel devices, a Section 513(g) request offers a unique opportunity to introduce a technology to the FDA, to familiarize the agency with that technology, and to suggest possible classifications, appropriate performance standards, and applicable regulatory requirements.

It allows for engagement with the relevant review division as the agency will often pose questions. And through those questions, it presents opportunities for insights into the agency's likely concerns about a new technology. This is all information that can be obtained relatively quickly because of the short statutory timeframe in which the agency is obligated to respond.

Submitters of 513(g) requests must pay a user fee to the agency, which for fiscal year 2022 was $5,061, but that is likely a small price to pay given overall development costs and the beneficial insights a response may yield.

Presubmission Meeting

Another way to engage the agency early is through a presubmission meeting.

According to the agency, "[a] Pre-Sub provides the opportunity for a submitter to obtain FDA feedback prior to an intended premarket submission."[2]

Through a presubmission meeting, a manufacturer can solicit information on a broader array of topics, including on the scope and scale of studies and testing and other data needed to support a submission.

A presubmission meeting request should include specific questions premised on specific proposals for the FDA to opine on. The agency will not want to design testing protocols from thin air, and a well-thought-out proposal is an opportunity to drive discussions and encourage FDA buy-in to studies that show reasonable safety and efficacy.

Feedback from the agency will likely be written, but meetings to discuss the offered feedback typically follow.

The insights and knowledge that can be gained from early engagement with the FDA can be invaluable to manufacturers of novel smart devices as they prepare study protocols and develop submissions.

A de novo classification request may ultimately prove the right answer for clearing a new technology, but the certainty about the proper approach for a submission that can come from agency feedback is often well worth the effort, particularly for newer devices without well-worn paths to market.

Privacy and Cybersecurity

Connecting medical devices to the internet, hospital networks or electronic instruments such as a smartphone or PC poses significant risks that require manufacturers to consider privacy and cybersecurity by design in order to limit cyber threats in the health care life cycle.

In addition to the significant concern that cybersecurity flaws could directly affect a patient's health, it is important to know that smart medical devices also increase the risk for ransomware attacks and data breaches.

A 2022 industry report by Cynerio and Ponemon Institute[3] found that 76% of ransomware-attacked hospitals were attacked three or more times and of those hospitals that were attacked, 24% noted a subsequent rise in their mortality rates. 43% of hospitals suffered a data breach in the past two years with average costs ranging from $1 million to $5 million and the largest data breach costing $13 million.

Smart medical device manufacturers should take a comprehensive approach to the development of their products, including the following:

Follow the recommended FDA guidance.

In April, the FDA issued a guidance document, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions."[4] The guidance provides recommendations regarding cybersecurity device design, labeling and the documentation. Some of the most important considerations include:

Comply with quality system regulation.

Device manufacturers should develop design controls that include software validation and procedures to allow for risk analysis.

Establish a secure development framework.

Secure development framework processes help reduce the number and severity of vulnerabilities in products and encompass all aspects of a product's lifecycle.

Design for security.

Throughout the development and manufacturing process, companies should keep the following security objectives in mind: authenticity (which includes integrity), authorization, availability, confidentiality, and the ability to timely and securely patch and update devices.

Track the software bill of materials.

Manufacturers can help reduce cybersecurity risk exposure by managing the weaknesses in the software stack.

The software bill of materials inventories software components during development and includes both the device manufacturer-developed components and third-party components. Third-party collateral can include purchased or licensed software as well as open-sourced software.

A software bill of materials will also include the upstream software dependencies required or depended on by proprietary, purchased or licensed, and open-source software. A software bill of materials or an equivalent capability should be maintained as part of the device's configuration management, and be regularly updated to reflect any changes to the software in devices.

Be on alert with the use of open-source software.

Because open-source software is developed by programmers who are usually outside of an organization, and is shared in the public space, manufacturers should assess potential vulnerabilities and how they can affect the overall function of the software and the device itself.

As demonstrated by the recent exposure of Log4j vulnerabilities,[5] manufacturers should be particularly mindful of components sourced from public libraries and incorporated into the software of medical devices.

Safeguard data when developing accompanying applications.

When developing applications that may accompany smart medical device products, manufacturers should evaluate areas of vulnerabilities of their application programming interfaces that allow communications with applications and databases to pass information back and forth. Data breaches involving protected health information may result in regulatory action and trigger obligations of nationwide or international data breach notification to impacted individuals.

Be aware of privacy legislation.

Many states' privacy and cybersecurity laws could affect smart medical device companies. Manufacturers should be aware of their potential implications for product development.

Manufacturers may also want to review the recently introduced American Data Privacy and Protection

Act,[6] a federal legislation aimed at creating a comprehensive federal consumer privacy framework. While not yet adopted, this may provide additional information of how privacy at the federal level may unfold in the coming years.

Privacy and cybersecurity flaws in smart medical devices can be costly to address, affect mortality and have a significant impact in the health care environment. Device manufacturers can move the needle on increasing the health and safety of patients by managing risks throughout the lifecycle of a smart medical device.

Summary

Smart medical device manufacturers are at the forefront of health care innovation.

Understanding intellectual property, regulatory, and privacy and cybersecurity issues associated with device development can significantly decrease the risk profile and potential liabilities throughout a product's lifecycle.

This will result in safer, more reliable products and more importantly, a positive contribution to addressing the health care needs of people around the world.

Anne Li and John Fuson are partners, and Gage Javier is an associate, at Crowell & Moring LLP.

[1] U.S. Food and Drug Administration, Guidance for Industry and Staff, FDA and Industry Procedures for Section 513(g) Requests for Information under the Federal Food, Drug, and Cosmetic Act, p.13 (Dec. 16, 2019).

[2] U.S. Food and Drug Administration, Guidance for Industry and Staff, Requests for Feedback and Meetings for Medical Device Submissions: The Q-Submission Program, p.3 (Jan. 6, 2021).

[3] The Insecurity of Connected Devices in Healthcare 2022, https://www.cynerio.com/insecurity-of-connected-devices-in-healthcare-2022?submissionGuid=f800af36-8605-4612-8cac-4df321d49102

[4] "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions." U.S Food and Drug Administration. Apr. 2022. Web.

[5] "Apache Log4j Vulnerability Guidance." Cybersecurity & Infrastructure Security Agency. n.d Web.

[6] "Overview of the American Data Privacy andProtection Act, H.R. 8152." Congressional Research Service. 31 Aug. 2022. Web.