DEPARTMENT OF HEALTH & HUMAN SERVICES Public Health Service

Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993

August 18, 2015

Ms. Jacqueline C. Charlesworth
General Counsel and Associate Register of Copyrights
United States Copyright Office
Library of Congress
101 Independence Avenue SE
Washington, DC 20559

Re: Section 1201 Rulemaking – Proposed Exemption for Medical Devices

Dear Ms. Charlesworth:

You sent a letter May 12, 2015, to FDA's Chief Counsel to inform FDA of a regulatory proceeding pending before the U.S. Copyright Office that relates to, among other things, medical devices. This is a rulemaking proceeding under 17 U.S.C. 1201 regarding potential exemptions to the general prohibition on circumvention of technological protection measures. You explained that one of the potential exemptions, relating to software in "networked medical devices," had been opposed by other rulemaking participants, who noted the FDA's regulatory authority for ensuring that medical devices are safe and effective. The potential exemption, filed by a coalition of medical device patients and researchers, would allow circumvention of TPMs in the firmware or software of medical devices and their corresponding monitoring systems. It covers devices such as pacemakers, implantable cardioverter defibrillators, insulin pumps, and continuous glucose monitors. You suggested that the FDA may have views concerning this matter.

Because this pertains to technical considerations for devices, my office was asked to respond. To the extent relevant to your regulatory proceeding, here are our views, which were prepared in consultation with FDA's Office of the Chief Counsel.

We note that while allowing circumvention of TPMs will not affect FDA's jurisdiction over products that continue to meet the device definition under 201(h) of the Federal Food, Drug, and Cosmetic Act (the FDCA) (21 USC 321(h)), and the entities that manufacture them, granting such an exemption for such devices could potentially create regulatory confusion for FDA, medical device manufacturers, and third party software developers that choose to modify medical devices.

1. Modifying or adding new software/firmware to a medical device already in commercial distribution may require the submission of a new premarket notification or premarket approval application.

Under the FDCA, products that meet the 201(h) definition of a device are required to have marketing authorization from FDA before being commercially distributed. Depending on the class of the device, which is based on risk, a person wishing to market a new device is, unless exempt, required to either submit a premarket notification under section 510(k) of the FDCA, 21 USC 360(k), or a premarket approval application (PMA) under section 515(a) of the FDCA, 21 USC 360e(a). The exemption, as we understand it, would allow third parties to circumvent the TPMs of devices that are within FDA's jurisdiction and are legally in commercial distribution. However, under FDA's regulations, a new premarket notification is required when a change or modification is made to a legally marketed device that that could significantly affect the safety or effectiveness of the device or changes/modifies the intended use of a device. See 21 CFR 807.81(a)(3)(i)-(ii). Similarly, a new PMA or PMA supplement is required when, among other things, changes are made to an approved device that affect safety and effectives or change the intended uses of the device. See 21 CFR 814.39(a).

From our discussion with Library of Congress staff, we understand the potential exemption to allow, among other things, third parties to access the software of medical devices that are currently on the market. From the discussion, it appears that it would be very difficult for third parties to fundamentally change the source code of the existing software, but it would be possible to add or modify software that expands and/or changes the intended uses of the device in ways that would, under the regulations cited above, require a new premarket notification or PMA be submitted to FDA before the modified device could be distributed.

Circumvention in this way may put third party developers in a position where, by virtue of modifying/adding device software, they would become the person responsible for obtaining marketing authorization (or an investigational device exemption (IDE) under section 520(g) of the FDCA, 21 U.S.C. § 360j(g)) before the modified device is distributed or used on patients. While it appears that, at least partially, the intent of exempting networked medical devices is to do lab/bench testing and research that does not involve or impact patients, the proposed rule specifically states that the exemption seeks to allow "circumvention of TPMs in the firmware or software of medical devices and their corresponding monitoring systems at *patient discretion.*" 79 FR 73871 (emphasis added).

The proposed rule asks whether a third party—rather than the owner of the device—may lawfully offer or engage in the proposed circumvention activities with respect to that device pursuant to an exemption granted under 17 U.S.C. 1201(a)(1). If FDA's understanding of the potential exemption is correct, it would appear that the answer could be no, at least in some circumstances. For example, if a third party were to modify the software of a device in a way that expands or otherwise modifies the intended uses or significantly affects safety and effectiveness of the device, and then offers the modified software to consumers without FDA marketing authorization, the third party would be in violation of sections 501(f)(1)(B) and 502(o) of the FDCA.

From a public health perspective, modified devices in distribution will cause confusion to users (patients, health care providers and caregivers) who may not be able to tell the difference between a modified device and an original device. Additionally, the users may have a difficult time in identifying the appropriate entity when attempting to obtain support and maintenance for such devices. Lack of clarity in determining the manufacturer and the functionality of the medical device can cause delays in timely resolution of malfunctions with a device and potentially lead to patient harm.

2. If a patient is injured by a device whose software has been modified, it may be difficult for FDA to determine responsibility from a medical device reporting standpoint.

Under section 519 of the FDCA, both manufacturers and user facilities[1] are required to submit a report to FDA when they receive or become aware of information that reasonably suggests that a device may have caused or contributed to a death or serious injury, or has malfunctioned in a way that similar devices are likely to cause or contribute to a death or serious injury. If the device's software has been modified by a third party, it may be much more difficult to understand how or why the device malfunctioned, and who is responsible for submitting a report to the FDA.

Similar to concerns expressed in the first point, third party developers may not understand that by modifying the functionality of a device, they have potentially stepped into the role of a device manufacturer[2] such that they would be required to meet not only the premarket authorization requirements described above, but postmarket ones as well, including reporting (21 CFR Part 803, Subpart E), quality system regulations (21 CFR Part 820), registration/listing (21 CFR Part 807 Subpart B), unique device identification (21 CFR Part 830), etc. These regulations are intended to, for example, correct adverse events and prevent adverse impact to public health. If a third party developer is not complying with these requirements, particularly premarket authorization and registration/listing requirements, device user facilities may submit the name of the original manufacturer in a report to FDA without knowing that the device had been modified. Furthermore, if a third party is subject to and not complying with the "unique device identifier" requirements (which provide for unique identification of each new version or model of a device), adverse events associated with the third party's new version or model may be improperly assigned to the previous version or model. From FDA's perspective, if the agency becomes aware that serious injuries are occurring from the use of particular device without knowing it has been modified, it may be difficult for the agency to ascertain the cause of the problem and to take appropriate actions to protect the public health.

---

[1] Device user facility means a hospital, ambulatory surgical facility, nursing home, outpatient diagnostic facility, or outpatient treatment facility as defined in this section, which is not a physician's office, as defined in this section. School nurse offices and employee health units are not device user facilities. 21 CFR 803.3.

[2] Manufacturer means any person who designs, manufactures, fabricates, assembles, or processes a finished device. Manufacturer includes but is not limited to those who perform the functions of contract sterilization, installation, relabeling, remanufacturing, repacking, or specification development, and initial distributors of foreign entities performing these functions. 21 CFR 820.3(o).

3. The exemption for software security research can have implications on human subject protections and related regulatory requirements.

Section III(G)(1) "Proposed Class 25: Software-Security Research" does not seem to make a distinction between bench top testing of device security and testing of a device in clinical use (i.e., an implant in an actual patient, a device in a hospital, etc.). These latter situations carry greater risk to patients and public health and may present challenges to FDA with respect to devices that have been manipulated (i.e., issues related to FDA's ability to hold manufacturers responsible once their device has been manipulated).

On October 1, 2014, the FDA released a final guidance for the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. The guidance recommends that manufacturers consider cybersecurity risks as part of the design and development of a medical device, and submit documentation to the FDA about the risks identified and controls in place to mitigate those risks. Based on the discussion with Library of Congress staff, one could interpret that including controls as part of the design can be considered TPMs. Circumventing these TPMs through the exemptions raises concerns from both regulatory expectations and public health perspective. The FDA notes that there could be risks and benefits of enabling "good-faith" research for the purpose of identifying, disclosing, and fixing malfunctions, security flaws, or vulnerabilities. For example, it could better harness the power of collaboration, in that if multiple stakeholders employ a common approach to identifying and mitigating cybersecurity vulnerabilities, the community at-large might benefit from a more efficient and thorough resolution of vulnerabilities. However, a risk to opening technology in this way is the difficulty for regulators and others to distinguish "good-faith" research efforts from malevolent third-party actors. In other words, leveraging the exemptions in the proposed rule could allow persons to gain unilateral access to proprietary software/source code to achieve objectives that might cause harm to public health, harm to specific patients, or compromise the data and systems that support these products in a healthcare setting.

In addition, from a regulatory perspective, this exemption may cause confusion for stakeholders that have been advised through FDA guidance to put appropriate cybersecurity controls in place to prevent third parties from manipulating the software of the device.

4. Other unintended public health concerns related to 3D printing, personal health information, and unlocking.

Regarding 3D Printing, manufacturers who utilize 3D printing to ultimately manufacture medical devices need to ensure that their products are safe and effective for their intended use. For example, if a 3D printed medical device is intended for insertion into the body, then the manufacturer under FDA regulations would have to demonstrate that the products are safe and effective for that intended use.

The proposed rule also refers to the term "data." If this term alludes to Patient Health Information (PHI), or Personal Identifiable Information (PII), then such information is regulated

by other Federal Institutions and Agencies. FDA strongly urges that these Institutions and Agencies are actively sought after for comment on the proposed rule.

Additionally, FDA would like to highlight Section III(c)(4) titled "Proposed Class 14: Unlocking – Wearable Computing Devices," which references the term "health monitoring devices," and Section III(c)(5) titled "Proposed Class 15: Unlocking – Consumer Machines," which references the terms "consumer machines" and "Internet of Things." Based on the information in the proposed rule, the FDA is unclear whether any of these terms include devices as defined in the FDCA (section 201(h), 21 USC 321(h)). Exemptions for such devices may have unintended public health consequences. For example, mobile phones and tablet computers appear to benefit from "unlocking" to provide consumers with access to the wireless networking marketplace. Conversely, by "unlocking" a medical device, one might actually modify the intended use of the product beyond the product's intended use, ultimately impacting the safety and effectiveness of the device.

We offer the following recommendations if the potential exemptions are finalized:

A. FDA recommends that the final rule explain that nothing in the rule will affect the regulation of products that fall within the jurisdiction of other federal agencies. As stated above, third parties that modify medical devices may become regulated manufacturers under the FDCA. As such, it may be useful for those who might circumvent TPMs to understand that other federal laws may apply and that the circumvention exemption is not an exemption from other applicable regulations.

B. We recommend that any final rule make a distinction between bench top testing of devices (where the unit tested is not in clinical use and will not be in clinical use in the future) and testing of devices during clinical use unless, for the latter, institutional review board (IRB) oversight is provided and investigational device exemptions (IDE) regulations are followed, as appropriate.

Thank you for informing FDA of this proceeding. Please let us know if you have any questions.

Sincerely yours,

Bakul Patel
Associate Director for Digital Health
Center for Devices and
Radiological Health