August 13, 2021

Kevin R. Amer
Acting General Counsel and Associate Register of Copyrights
United States Copyright Office
Library of Congress
101 Independence Avenue SE
Washington, DC 20559

Sent via email: kamer@copyright.gov

Re: Section 1201 Rulemaking – Proposed Exemptions Pertaining to Medical Devices

Dear Mr. Amer:

On May 4, 2021, Regan A. Smith, General Counsel and Associate Register of Copyrights for the United States Copyright Office, sent a letter to FDA's Acting Chief Counsel to inform FDA of a rulemaking proceeding pending before the Copyright Office that relates to, among other things, medical devices. We understand that this proceeding pertains to 17 U.S.C. § 1201 and potential exemptions to the general prohibition on the circumvention of technological protection measures (TPMs) that control access to copyrighted works, including software. Ms. Smith stated that participants in the rulemaking process had referenced FDA's regulatory authority in this area as relates to the safety and effectiveness of medical devices, and the Copyright Office therefore sought to make FDA aware of the rulemaking proceeding.

Ms. Smith drew FDA's attention to two proposed exemptions being considered in this proceeding. The first of these proposed exemptions, designated the "Class 9" proposal, seeks to expand an existing exemption under 37 C.F.R. § 201.40(b)(4), pursuant to which the prohibition on circumventing TPMs does not apply to a patient who accesses compilations of data generated by the patient's own medical device or corresponding personal monitoring system, provided that the device is wholly or partially implanted in the patient's body; the circumvention is undertaken by the patient; the access is accomplished through the passive monitoring of wireless transmissions already being produced by the device or monitoring system; and the circumvention does not constitute a violation of applicable law. The Class 9 proposal would remove these four limitations.

Under the second proposed exemption, designated the "Class 12" proposal, the prohibition on circumventing TPMs would not apply to circumvention that is conducted to access computer programs and data files that are contained in and control the functioning of medical devices (among other things) for the purpose of diagnosis, maintenance, or repair of such devices. Ms. Smith stated that opponents of both proposals have expressed concerns regarding potential impacts to health and safety should the exemptions be granted.

FDA would like to thank the Copyright Office for informing FDA of this proceeding. The following are

our views with respect to both the Class 9 and Class 12 proposals, as they relate to devices within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act (referred to as "medical devices" herein). We offer no opinion at this time on any existing exemptions or proposed exemptions to the general prohibition on the circumvention of TPMs that control access to copyrighted works other than as specifically discussed below.

Class 9

It is FDA's understanding that the proposed expansion of the current exemption under 37 C.F.R. § 201.40(b)(4) would broaden opportunities for patients to access data generated by their own medical devices without potential liability under 17 U.S.C. § 1201, but would impose no requirements on, or in any way limit the actions of, the manufacturers of those devices. FDA does not believe that further exempting patients (or those acting on their behalf) from potential liability in this fashion is likely to significantly impact the safety or effectiveness of medical devices, or to impair the ability of medical device manufacturers to comply with applicable regulatory requirements enforced by FDA. We are aware that opponents of the proposed expansion have raised concerns that the expansion may jeopardize the cybersecurity of affected devices, and may require greater effort from manufacturers to ensure that their devices remain secure. FDA believes that an exemption from liability expressly limited to circumvention conducted for the sole purpose of lawfully accessing data generated by a patient's own device or associated monitoring system, whether or not such device is implanted and/or such access is accomplished through the passive monitoring of existing wireless transmissions, is unlikely to undermine the cybersecurity of affected devices, other than as intentionally undertaken by the patient and as may impact only such patient's own device. FDA further believes that the proposed expansion of the exemption under 37 C.F.R. § 201.40(b)(4) is broadly consistent with the existing exemption for good-faith security research under 37 C.F.R. § 201.40(b)(11). FDA therefore does not view the proposed expansion of the exemption at 37 C.F.R. § 201.40(b)(4) as likely to undermine or impede efforts to ensure an appropriate degree of cybersecurity for medical devices.

FDA notes that the Class 9 proposal includes modifications to 37 C.F.R. § 201.40(b)(4) that would remove the current regulatory language expressly limiting the exemption to circumvention that "does not constitute a violation of applicable law, including without limitation the Health Insurance Portability and Accountability Act of 1996, the Computer Fraud and Abuse Act of 1986 or regulations of the Food and Drug Administration." To the extent this language is removed from the regulation, FDA recommends that the final rule clarify that nothing in the rule affects the application of other federal laws and regulations, and remind interested parties that the exemption continues to apply only where circumvention is undertaken "for the sole purpose of *lawfully* accessing the data generated by [the patient's] own device or monitoring system" (emphasis added).

Class 12

As a preliminary matter, FDA understands that the proposed exemption would apply to circumvention that is conducted solely to obtain data access for the purpose of diagnosis,

maintenance, or repair of medical devices, and not for the purpose of device modification that may significantly change the performance or safety specifications of the device or its intended use.[1] FDA further understands that opponents of the Class 12 proposal have expressed concerns that the exemption may facilitate device servicing by unregulated entities, with the potential to increase cybersecurity risks and result in harm to both patients and providers.

In May 2018, FDA issued a report that evaluated the available evidence pertaining to the quality, safety, and effectiveness of medical device servicing in the United States.[2] Based on an assessment of complaints, peer-reviewed published literature, medical device reports describing suspected device-associated deaths, serious injuries, and malfunctions, and research and analysis provided by third parties, the report concluded that many entities that perform or participate in the servicing of medical devices – including both original equipment manufacturers (OEMs) and independent service organization (ISOs) – provide high quality, safe, and effective medical device servicing.[3] The report determined that the available evidence was insufficient to conclude whether or not there is a widespread public health concern relating to medical device servicing, and therefore concluded that the evidence did not justify imposing additional regulatory requirements on ISOs.[4] The report further concluded that the continued availability of ISOs to service and repair medical devices is critical to the functioning of the healthcare system in the United States.[5]

With respect to cybersecurity concerns in particular, FDA recently issued a discussion paper that is intended to guide future assessment of both the challenges and opportunities related to cybersecurity and the servicing of medical devices.[6] The discussion paper acknowledges the cybersecurity challenges related to ISO servicing of medical devices, but also notes that device servicing entities may be well positioned to help identify and address security vulnerabilities, and observes that ISOs may play an important role in maintaining the overall quality, safety, and efficacy of medical devices. FDA therefore does not share the view that an exemption from liability under 17 U.S.C. § 1201 for circumvention conducted solely for the purpose of diagnosis, maintenance, or repair of medical devices would necessarily and materially jeopardize the safety and effectiveness of medical devices in the United States with respect to cybersecurity; however, FDA has sought stakeholder input on this topic and is evaluating FDA's approach to cybersecurity and medical device servicing.

---

[1] FDA notes that if the proposed exemption were to cover device modification that may significantly change the performance or safety specifications of the device or its intended use, such exemption could raise safety and effectiveness concerns not addressed in this letter, and may have implications with respect to the application of FDA regulatory requirements pertaining to device marketing authorization, registration/listing, quality system regulations, and medical device reporting, among other requirements.

[2] "FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices," available at https://www.fda.gov/media/113431/download.

[3] *See id*. at 23.

[4] *Id*.

[5] *Id*.

[6] "Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities," available at https://www.fda.gov/media/150144/download.

Please let us know if you have any questions regarding these comments, or if FDA can be of any further assistance to the Copyright Office in connection with this rulemaking proceeding.

Sincerely,

Suzanne B. Schwartz -S

Digitally signed by Suzanne B. Schwartz -S
Date: 2021.08.13 11:12:55 -04'00'

Suzanne B. Schwartz, MD, MBA
Director, Office of Strategic Partnerships and Technology Innovation
Center for Devices and Radiological Health
U.S. Food and Drug Administration