Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201
[Docket No. 2014–07]

Advanced Medical Technology Association Comments Regarding
Proposed Class 27: Software – Networked Medical Devices

No Multimedia evidence is being provided in connection with this comment.

ITEM 1. COMMENTER INFORMATION

The Advanced Medical Technology Association ("AdvaMed") is the world's largest association representing manufacturers of medical devices, diagnostic products, and health information systems that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatments. Our members produce nearly 90 percent of the health care technology purchased annually in the United States and range from the smallest to the largest medical technology innovators and companies.

Advanced Medical Technology Association (AdvaMed)
701 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20004
legal@advamed.org

ITEM 2. PROPOSED CLASS ADDRESSED

These comments concern Proposed Class 27: Software—Networked Medical Devices.

ITEM 3. OVERVIEW

The proposed exemption should be rejected for a number of reasons, including:

(1) patient safety and privacy will be placed at risk through the requested exemption;
(2) robust medical device security research is already ongoing under a framework that includes the necessary protections for patient privacy, patient safety, and intellectual property;
(3) the FDA should retain regulatory supremacy over device operations;
(4) the exemption, if granted, would create incentives to misuse devices; and
(5) the scope of the class subject to the exemption is so broad as to make a full and comprehensive assessment of the risks created, if the exemption were granted, almost impossible to measure.

1. **Any unauthorized circumvention activity lacks necessary protections for patient safety and privacy.** Where patients seek to circumvent the Technological Protection Measures ("TPMs") of devices that are implanted or attached to their person, as this activity would be outside of the manufacturer's design, there is the very real possibility a device malfunction could result, unnecessarily jeopardizing

the safety of a patient. This is particularly concerning for implanted networked medical devices (e.g., pacemakers or ICDs) and attached medical devices (e.g., insulin pumps or glucose monitors), as this activity may profoundly change a device's operation, resulting in injury or death. Further, circumvention attempts will cause these devices to switch into a communication mode, increasing power consumption and accelerating battery drain, resulting in more frequent surgical replacements of the device along with the associated potential for surgical complications. For example, in some implanted networked devices, battery drain during telemetry can be 500 times greater than during standard operation. Under those circumstances, every 1 hour of telemetry would reduce the longevity of the device by 1.5 weeks. The longevity estimates for some devices are based on the assumption that telemetry usage per year will not exceed 1.5 hours per year. This translates to a 3-6% battery allocation for wireless telemetry use. Allowing a patient to regularly download data from their implanted devices would adversely impact the longevity of their devices. In addition to concerns about the excessive frequency of data downloads, patients may unintentionally leave the telemetry session on for extended periods of time. It would take just a few days of continuous telemetry use to fully drain the battery.

We believe that patients have the inherent right to access their own medical data, however this in and of itself does not necessitate bypass of any intellectual property protections. Patients directly accessing the data on their devices may not understand the format of the data or may misinterpret the data. Such data access rights can be exercised (and already are provided) through health care providers having the appropriate tools and training to collect and protect patient data without compromising the safety and longevity of his or her device.

Further, where unauthorized circumvention activity is utilized to access the corresponding monitoring system of an implanted or attached device, or its associated networked systems, patient personally identifiable (PII) or protected health information (PHI) of other patients may be compromised.

2. **Robust medical device security research is already ongoing under a framework that includes the necessary protections for patient privacy, patient safety, and intellectual property.** The proposed exemption purports to address a problem which, in fact, is already being widely worked on by industry. In particular, medical device manufacturers have been and are presently engaged with technology companies and academic researchers to evaluate the security, safety and efficacy of medical devices. The appropriate framework to evaluate medical device security is through formal agreements with researchers that include the necessary protections for patient privacy, patient safety, and intellectual property. Recently, the U.S. Food and Drug Administration ("FDA") sponsored a well-attended workshop among industry, academic and government leaders (including at least one of the petitioners, Jay Radcliffe of Rapid7) entitled "Collaborative Approaches for Medical Device and Healthcare Cybersecurity" See http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM419427.pdf and other workshops are scheduled in the near future. See

also "Software and Cybersecurity Risk Management for Medical Devices", scheduled for May 11-12, 2015. See http://www.fdanews.com/cybersecuritymd. Moreover, established institutes focus on device security, such as the Archimedes Institute at the University of Michigan ("Archimedes focuses on research and education to improve medical device security"), which conducts ongoing device cybersecurity research in partnership with many industry leaders. See http://www.secure-medicine.org.

After the initial demonstration of a patient getting access to an insulin pump, the industry has responded robustly. At least one industry leader is reported to have hired three separate security firms to conduct research. See http://www.bloomberg.com/news/articles/2012-02-29/mcafee-hacker-says-medtronic-insulin-pumps-vulnerable-to-attack. ("Medtronic has responded to the risks by hiring security teams from three organizations to inspect its products.") In short, medical device cybersecurity research is ongoing, active and well supported by industry and government. With these public efforts by device manufacturers to work with FDA and academia to improve and collaborate on security, there would seem to be little factual support to the petitioners' statement: "Such research is rarely if ever done with the manufacture consent or authorization, no doubt in part due to the fact that discovery of flaws could lead to costly recalls, FDA investigations, and class-action lawsuits." See Petition. See http://copyright.gov/1201/2014/petitions/Berkman_Center_1201_Initial_Submission_2014.pdf. This particular exemption request might be merely a showpiece - meant to drive market awareness of the researchers' abilities and availability.

3. **FDA should retain regulatory supremacy over medical device operations.** As FDA is the responsible federal agency to assure the safety, efficacy and security of medical devices, we respectfully request that the Copyright Office oppose the creation of an exemption for Proposed Class 27 and defer to FDA management of the framework to further research on the safety, efficacy and security of medical devices. Circumvention activity without oversight by FDA and without a manufacturer's consultation will endanger patients.

   FDA has recognized that access to the proprietary software code is not necessary for the evaluation of safety and efficacy. The U.S. government has communicated this point to foreign regulators in countries associated with counterfeiting activities who have demanded access to the code for the supposed evaluation of safety and efficacy. Creating this exemption would encourage these demands and weaken the U.S. government's arguments to stand up to these countries.

   If the Copyright Office were to advance an exception permitting unauthorized circumvention activity for a patient to study his or her own device, it should be limited to the passive monitoring of radio transmissions that are produced by the device in its unaltered operating form. No unauthorized engagement or manipulation of the device or its reader should be permitted via radio signal or otherwise if the device is or will be used for patient care in the future, as the risk of damage and degradation of the device outweighs the "benefit" of making these

devices available to researchers who do not wish to enter into formal research agreements.

4. **The exemption, if granted, would create incentives to misuse devices for unintended purposes and thereby misuse device manufacturer's back-end systems.** Device programmers (for communication with implanted devices and home monitors) automatically transfer information to the device manufacturer's back-end systems which, in turn, permit the information to be transferred to the patient's doctor. Triggering multiple additional transmissions to track the encoding will quite likely cause the system to automatically send information to those systems. This is an unauthorized use of the device manufacturer's systems, which are meant for patient care, also raising HIPAA concerns. Moreover, in many states, unauthorized access to computer systems is a crime. So the exemption could very well provide a perverse incentive for people to make unauthorized, and sometimes illegal, use of the device manufacturer's systems.

5. **The proposed exemption is overly broad.** The proposed exemption allows for "circumvention of TPMs protecting computer programs in medical devices designed for attachment to…patients." The scope of the would include many more devices other than those specified, including cochlear implants, powered prostatic joints[1], deep brain stimulators, and various types of ambulatory devices. This exemption is overbroad since it could potentially cover devices that are "attached" to patients temporarily (e.g., fluid delivery mechanisms) but do not receive any feedback data, as well as devices that are indirectly attached to patients (e.g., connected to a device that is directly attached to a patient). With this broad spectrum of additional devices within the class, it is difficult to appraise the full scope or risks likely to be created. If an exemption were to be granted, we request that it be narrowly tailored to remove any ambiguities and adequately address all risks. In fact, circumvention activity should not be permitted for any implanted or attached device that is currently, or may in future be, utilized for the clinical care of patients due to unnecessary risks to patient safety and privacy. Tampering with any implanted devices presents an unnecessarily high risk to patient safety due to the malfunction, degradation, and/or damage that may result from unauthorized circumvention activity with these devices. Circumvention in these instances may result in malfunctions after the device has been reattached to a patient and / or corrupt the data that the prescribing physician is depending on to determine treatment. Unauthorized circumvention of corresponding monitoring devices of some implanted or attached devices will compromise the personal health

1 See http://www.businesswire.com/news/home/20120905006102/en/Technology-Breakthrough-Prosthetic-Device-Connects-Patients-Health ("Another innovative feature is Magellan's connectivity, linking the device to its user and the user's health care providers. This functionality, afforded by iPhone and iPad apps and Bluetooth technology, enables patients to make adjustments to the Magellan themselves, such as adaptations to account for changes in footwear. This functionality also extends to health care providers, affording access to patient performance and device diagnostics. 'We are living in a connected, digital world,' commented Orthocare Innovations' CEO and Co-Founder Doug McCormack")

information of other patients who have not consented to such a study for security purposes or otherwise.

ITEM 4. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

The methods of circumvention to access the code in an implanted or attached device often requires the type of experimentation that should not be conducted on devices used in patient care. In general, a patient would not retain a formerly implanted device or attached device that is no longer being used for his or her own care.

Typically, the TPMs used in medical devices includes data encryption that requires a key to the encryption in order to understand the data. In addition, passwords may be used to limit access to the medical device. TPMs have been implemented by medical device manufacturers to protect patient data that is protected by HIPAA, to protect patient safety and to protect the intellectual property (copyright/patents/trade secrets) incorporated into the medical device.

ITEM 5. ASSERTED NONINFRINGING USE(S)

Any arguably noninfringing uses of the copyrighted work gained by unauthorized circumvention of TPMs presents unnecessary risk to patient safety when conducted on devices that are or may be used in the future for clinical care. The Notice discusses medical device outputs, and asks whether such outputs can constitute copyrightable subject matter. While such a determination is fact specific, copyright protection in device outputs may extend to, for example, the structure, format, and arrangement of the output data. *See Engineering Dynamics, Inc. v. Structural Software, Inc.*, 26 F.3d 1335, 1345 (5th Cir. 1994) (holding that user input/output formats are protectable); *Positive Software Solutions, Inc. v. New Century Mortgage Corp.*, 259 F. Supp. 2d 531, 535 (N.D. Tex. 2003) (holding that SQL data structures meet the requisite degree of creative expression). Accordingly, to the extent that device outputs constitute copyrightable subject matter, the only noninfringing use would have to qualify under the fair use doctrine, as discussed below. This would also be necessary for the analysis of asserted noninfringing uses of protectable source code.

The analysis of any use of the copyrighted works arguably points against the proposed uses falling under the fair use exception. For example, a four pronged test for fair use has been codified. The prongs include the character of the use, the nature of the copyrighted work, the portion of the copyrighted work used and the effect of the use on the value of the copyrighted work[2].

Is the exemption being requested for the profit of the petitioners? The character of use is arguably for the profit of the group of individuals making up the coalition that is requesting the exemption. In the past, some of the members of the coalition have created public

2 17 U.S.C. § 107

hysteria around gaining access to medical device.[3,4] In turn, these individuals have used accessing the copyrighted works of medical devices for profit.[5,6] Due to the public hysteria, these researchers have approached the medical device manufacturers to offer paid consulting services in relation to the security of the medical devices. Since, in the past, the uses of the copyright works have been for profit, this prong of the use exemption points against the use being a fair use of the copyrighted work. At least one of the petitioners works for a major cyber security firm, Rapid7 ("Rapid7's mission is to engineer simple, innovative solutions for security's critical challenges"). See http://www.rapid7.com/company/index.jsp.

Is the requested exemption for a small portion of the copyrighted work for or for the entire work? For this particular exemption, the researchers seek to use the entire portion of the copyrighted work and all the data from the medical device. The researchers want to use everything. They have asked to be allowed to reverse engineer any software or source code, and they have asked for access to all data from the medical devices. Courts have typically required small portions of the copyrighted work to be used in order for the use to be considered a fair use. As a result, since the exemption has asked for use of the entire copyrighted work, this prong points against the use being a fair use of the copyrighted work.[7]

The courts have found that these prongs are not dispositive of the fair use analysis.[8] However, even with the defendants (likely the researchers) having the burden of proof when asserting that the use of the copyright fair use[9], weighing the four prongs likely point against the use of the copyrighted work being a fair use.

---

3 Jay Radcliffe, *Hacking Medical Devices for Fun and Insulin; Breaking the Human SCADA System*," Black Hat Convention (August 2011), (accessed March 2015) – https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf (The author outlines a "Theoretical Insulin Pump Attack" where the medical device could be manipulated by a hacker to, "cause the receiver unit to indicate a higher sugar reading then [sic] actually exists", and the author also writes that through hacking "[a] diabetic could be manipulated into administering more insulin then [sic] needed, potentially causing a hypoglycemic condition.").

4 Jim Finkle, *Rapid7 hires Jay Radcliffe, diabetic who hacked his insulin pump*, REUTERS (May 29, 2014), (accessed March 2015) http://www.reuters.com/article/2014/05/29/us-rapid7-radcliffe-idUSKBN0E929K20140529 ("He [Radcliffe] said the approach could have been used to deliver lethal doses of insulin to patients.").

5 Julie Appleby and Daniela Hernandez, *Can Hackers Get Into Your Pacemaker?*, THE ATLANTIC (Nov. 20, 2014), http://www.theatlantic.com/health/archive/2014/11/can-hackers-get-into-your-pacemaker/382893/. (The first sentence of the article reads "Jay Radcliffe breaks into medical devices for a living...").

6 See Finkle, *supra* note 3 ("Rapid7 ... hired Jay Radcliffe ... known for ... hacking his own insulin pump.").

7 *Id.*

8 Swatch Grp. Mgmt. Servs. Ltd. v. Bloomberg L.P., 756 F.3d 73 (2d 2014).

9 *Id.*

ITEM 6. ASSERTED ADVERSE EFFECTS

Alternatives that do not require unauthorized circumvention to study the safety, efficacy and security of medical devices exist in the form of formalized research agreements that ensure the protection of patient safety, patient privacy and intellectual property.

The proposed exemption would negatively impact the security of medical devices, even with respect to devices that will never be used with a patient. For example, allowing for the circumvention of TPMs in medical devices could provide wrongdoers with knowledge of how to manipulate and interface with the devices to cause harm to patients. The dissemination of proprietary methodologies and information garnered by reverse engineering such devices and their outputs will enable wrongdoers to manipulate and/or invade other devices that are in-use (or will be used) to the possible detriment of patients.

In addition to the underlying copyright concerns relating to device firmware and outputs, the proposed exemption also poses trade secret concerns. Pursuing formal channels of research, by requesting authorization from manufacturers to test and reverse engineer medical devices, allows for manufacturers to secure contractual protections to maintain their trade secrets. In many cases, trade secrets may be the only viable form of protection for companies conducting research and development in this area.

Other concerns include violation of privacy rights. In certain instances, networked devices could be used to access information which third parties should not be able to access and/or monitor. Further, these privacy violations could impact how insurance carriers evaluate their patients and claims.

The Notice asks for commentary on whether the exemption, if granted, should distinguish among different users. If such an exemption is permitted, we believe that there should be narrow categories of permitted activities that are specific to each type of user. For example, if the user is a patient, the patient's exempted circumvention could be limited to examining the output of his or her own device. If the user is a researcher, the exempted circumvention could be limited to studies on device efficacy. An overbroad exemption presents numerous risks of patient safety and privacy.

ITEM 7. STATUTORY FACTORS

As it has occurred in the past, publicity related to accessing a patient's medical device creates fear in the public and in the patient because they worry that their devices will be accessed or controlled. This fear can, and has, led to patient panic (especially in the elderly), and causes the public to believe that these life-saving medical devices are not safe or secure. As a result, some patients will not seek the medical treatment that will improve their quality of life.

This proposed exemption implicates life-saving medical technologies. In view of the profound risks associated with unauthorized circumvention, we strongly believe that the Copyright Office should confer with FDA and defer to its views in this matter, as FDA is the federal agency charged with assuring the safety, efficacy and security of medical devices.