Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201
Docket No. 014-07

Advanced Medical Technology Association & Medical Imaging and Technology Alliance Joint Comments Regarding
Proposed Class 25: Software—Security Research

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

The Medical Imaging and Technology Alliance ("MITA") is the leading organization and collective voice of medical imaging equipment, radiation therapy and radiopharmaceutical manufacturers, innovators and product developers. It represents companies whose sales comprise more than 90 percent of the global market for medical imaging technology. MITA is a division of the National Electrical Manufacturers Association.

MITA
1300 North 17th Street
Suite 900
Arlington, VA 22209
MITA@medicalimaging.org

ITEM 2. PROPOSED CLASS ADDRESSED

These comments concern Proposed Class 25: Software—Security Research

ITEM 3. OVERVIEW

For the reasons stated below, we respectfully request that the Copyright Office oppose the inclusion of medical devices in an exemption under Proposed Class 25.

Position Summary

- Allowing unauthorized circumvention of TPMs in medical devices can harm patients, compromise patient privacy, and place valuable intellectual property at risk.
- Permitting unauthorized circumvention for security and vulnerability research or to "fix" medical devices without oversight by FDA and without a manufacturer's consultation will endanger patients and conflicts with the existing regulatory framework.
- Robust medical device cybersecurity research is already ongoing under a framework that includes the necessary protections for patient privacy, patient safety, and intellectual property.
- The exemption, if granted for medical devices, may also negatively impact innovation, health care costs, and supply chain integrity.
- An exception in Copyright protections is not required for patient safety, for continued improvement of security in Medical Devices, or for safely providing patients with access to their device data.

Commentary

As a general matter, while the proposed exemption is limited to researchers seeking to perform "good faith testing, identifying, disclosing and fixing of malfunctions, security flaws, or vulnerabilities," this language is very broad and open to interpretation. Such an exemption, as applied to medical devices, will do more damage than good. The proposal eliminates the proper and controlled frameworks in place that afford appropriate research and testing of medical technologies without compromising patients and intellectual property.

I. Allowing unauthorized circumvention of TPMs in medical devices can harm patients, compromise patient privacy, and place valuable intellectual property at risk.

Where researchers seek to circumvent the Technological Protection Measures ("TPMs") of devices that are currently or may in the future be used for patient care, the risk of damage, malfunction, degradation, and/or data corruption and the associated potential harm to patient safety outweighs the benefit offered by unauthorized security research. Such an exemption would also place patients' personal health information at risk and would contravene federal and state privacy laws concerning the storage and transmission of protected health information ("PHI")—such as requirements for certain levels of encryption, as well as the development of policies and measures to ensure the safekeeping of PHI.

As circumvention activities 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 concerning for networked medical devices such as implants containing software, software used in Radiology imaging and distribution systems, Software used for planning of radiation treatments, for example, as this activity may profoundly change a device's operation resulting in injury or death. Circumvention attempts drain the finite battery charge within an implanted networked medical device—these 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 implanted 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. Further, where unauthorized circumvention activity is utilized to access the corresponding monitoring system of an implanted or attached device, or networked patient imaging and health record systems, the privacy and personal health information of other patients may be compromised.

Allowing circumvention activities would lead to exposure of medical device source code and patient data. Having access to that information would provide the details of how the medical device operates, and how patient data is processed and stored. The unintended or malicious release of that information to inappropriate parties could lead to malicious attacks to do patients harm, interrupt device operation or change configuration, or loss of patient personally identifiable (PII) or protected health information (PHI).

II. Permitting unauthorized circumvention for security and vulnerability research or to "fix" medical devices without oversight by FDA and without a manufacturer's consultation will endanger patients and conflicts with the existing regulatory framework.

As the U.S. Food and Drug Administration ("FDA") is the federal agency responsible for assuring the safety, efficacy and security of medical devices, we respectfully request that the Copyright Office oppose the inclusion of medical devices in an exemption under Proposed Class 25 and defer to FDA management of the framework to further research on the safety, efficacy and security of medical devices. The copyrighted medical devices subject to the proposed rulemaking are generally not publicly available and in most cases are indicated for prescription use or for use by the order of a physician in accordance with Section 201 of the Federal Food, Drug and Cosmetic Act (FD&C Act).

Allowing access to the source code of a medical device presents a regulatory and quality issue since the information being accessed is regulated by the FDA. Any access to, reverse engineering of, or change in the source code of a medical device should be overseen by the FDA. Including medical devices in the exemption seemingly usurps the authority of the FDA to regulate medical devices for patient safety, efficacy and security.

The proposed exemption is in stark contrast and circumvents FDA's regulatory thinking and position outlined in its guidance to medical device manufacturers' encouraging the use of mechanisms such as locks and TPMs to thwart cybersecurity threats (Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff; October 2, 2014; U.S. Department of Health and Human Services Food and Drug Administration Center for Devices and Radiological Health).

Based on FDA enforced Current Good Manufacturing Practice (21 C.F.R. Part 110), Quality Systems Regulations (21 C.F.R. Part 820), software validation and risk analysis (required by 21 C.F.R. § 820.30(g)), and FDA guidance (Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, October 2014) all medical devices containing software have undergone extensive security testing and evaluation prior to seeking FDA approval. These requirements are often met by submitting a device to an independent security testing lab (researchers) for evaluation under a contractual agreement. End users may also request a Manufacturer Disclosure Statement for Medical Device Security (HIMSS/ NEMA MDS2 form) which can aid in their individual assessment of the vulnerabilities and risks associated with protecting the health information created, received, transmitted or maintained by a medical device.

Any provision of code for unauthorized use, including for non-licensed purposes such as "reverse engineering", contravenes contractual law, current copyright laws, and public policy. Circumvention exceptions proposed in the rule would subject medical device license-holders to losses of intellectual property, potential liabilities for harm, and increase recall and reporting requirements to FDA. This loss of IP rights and increased potential for liabilities could stifle overall investment in medical technology. Under the FD&C Act medical device manufacturers remain responsible for the safety of their devices even after they have been entered into commerce and altered by a third party. This includes reporting requirements under the Electronic Product Radiation Control Program (x-rays, ultrasound, radio waves etc.) when equipment fails to accomplish its intended purpose. Unauthorized security testing is generally intended to cause a device to fail or otherwise alter its ability to function as intended, because unauthorized testing must necessarily be conducted on a device already entered into commerce, manufacturers would be required to file a report or single-system recall based on the danger presented by the now corrupted device.

At the behest of developing international standards, global governmental agencies, and the healthcare industry (providers and medical device manufacturers), significant investments which include the use of independent test agencies and consultants specializing in security and cybersecurity, the adoption of best practices and active engagement with regulators to advance security protections of medical devices have been and continue in an environment of threat unpredictability.

Further, allowing circumvention of TPMs to "fix" medical devices without manufacturer or FDA permission should not be permitted. The requested exemption "would allow researchers to circumvent access controls in relation to computer programs, databases, and devices for purposes of good-faith testing, identifying, disclosing and fixing of

malfunctions, security flaws, or vulnerabilities." Fixing medical devices, without FDA oversight and without manufacturer's consultation is unwise and will risk patient safety. Medical devices are highly engineered, well-tested products which very often a patient's life depend upon. FDA oversees the design and use of these products with great rigor, and often requires extensive clinical studies to establish safety and efficacy. The granting of the exemption would enable others to bypass proper regulatory controls, and ultimately risk patent health through any so-called "fix."

The proposal erodes the proper and controlled frameworks in place that afford appropriate research and testing without compromising patient safety and patient privacy, as well as, the safety, efficacy and security of medical devices.

III. Robust medical device cybersecurity research is already ongoing under a framework that includes the necessary protections for patient privacy, patient safety, and intellectual property.

Medical technology manufacturers have been and are presently engaged with technology companies and academic researchers to evaluate the security of devices and make changes to design. The proper 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. For example, 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. Any unauthorized circumvention activity lacks these necessary protections.

IV. The exemption, if granted for medical devices, may also negatively impact innovation, health care costs, and supply chain integrity.

Allowing circumvention activities would lead manufacturers to invest a greater percentage of finite resources into bolstering access controls or other TPMs to ensure the protection of intellectual property and patient safety. The result would be a reduction of a manufacturer's capability for innovation that improves healthcare.

Allowing access to the source code in medical devices without consent and without following the manufacturer's instructions could lead to attacks or misuse that cause medical devices to malfunction. With the litigious nature of society, any medical device malfunction is highly likely to result in a products liability suit for the medical manufacturer. These claims will increase the legal costs for the medical manufacturer.

Without research agreements to protect intellectual property, manufacturers will be concerned about the disclosure of the trade secret aspects of the code and its accessibility to counterfeiters. Allowing circumvention activities that expose the source code in a medical device encourages theft of trade secrets and the infringement of patents since most source code is either patented or considered to be a trade secret by medical device manufacturers.

In addition, allowing access to and reverse engineering of source code would likely increase the number of knock-off products, because once the source code is obtained it could easily be transmitted to anyone in the world or posted on the Internet. This could lead to the production of black market devices that would be difficult to track and or distinguish from the legal or legitimate manufactured products.

Allowing circumvention activities that provide access to the source code and patient data without the consent of the copyright owner will encourage malicious actors to access medical devices and their data without the consent of the patient. Nothing in the proposed exemption discusses patient consent when accessing the medical device's data and/or source code. This highly sensitive information could be used to harm patients and, without formalized agreements in place to allow for sanctioned security research, there will be no accountability for the disclosure of such information.

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.

Researchers exposing the reverse engineering (circumvention) techniques for defeating existing technological protections could result in those techniques being used on many kinds of technologies across multiple industries.

V. An exception in Copyright protections is not required for patient safety, for continued improvement of security in Medical Devices, or for safely providing patients with access to their device data.

We agree that providing a method for patients to access their device data is favorable. As healthcare moves quickly to providing patients with the ability to actively manage their own healthcare, we believe that market demand, regulatory requirements and changes in healthcare will inevitably require manufacturers and healthcare delivery organizations to establish safe methods for access to that information. However, it must be provided in a structured, consistent, secure, safe, reliable and approved way. Gaining access to that data via circumvention activities does not satisfy or guarantee any of those requirements.

Without having those provisions in place, patients would not be guaranteed that the data is reliable, could misinterpret data, or may not understand the format of the data. Any of these circumstances could lead to incorrect decisions about their healthcare. The risk of losing patient PII and PHI would also increase.

Conclusion

Very serious health care issues that could adversely affect patients and confidence in medical devices will arise if the exemption is granted.

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

The following are examples of the Technical Protection Measures used on Medical Devices, and how they may be circumvented. This list is not exhaustive, and not all TPMs may be applicable or required for each device type.

Limit Access to Trusted Users Only

- Technical Protection Measures that ensure secure communications with the device using strong encryption and authentication.
- Limit access to use or communicate with devices through the authentication of users (e.g. user ID and password, smartcard, biometric, or digital certificates). If digital certificates used for strong authentication are not stored in a highly secure manner, it may be possible to compromise and use them to improperly gain access to the device.
- Use automatic timed methods to terminate sessions within the system where appropriate for the use environment;
- Controlling and limiting the times that the device is able to communicate to reduce the window for possible attacks. If a researcher or malicious actor is able to observe and monitor the activity of the device through circumvention activities, the actor could determine when or under what conditions the device is available for communications.
- Encryption data on the device. If the schema for encrypting data on the device is not sufficiently complex, or that schema has been compromised by others before, circumvention activities may be possible to "un-encrypt" and view the data. Additionally, if the digital key that contains the encryption details is not sufficiently protected and exposed by circumvention activities, encryption can be bypassed.
- Where appropriate, employ a layered authorization model by differentiating privileges based on the user role (e.g. caregiver, system administrator) or device role;
- Use appropriate authentication (e.g. multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel);
- Strengthen password protection by avoiding "hardcoded" password or common words (i.e. passwords which are the same for each device, difficult to change, and vulnerable to public disclosure) and limit public access to passwords used for privileged device access;
- Where appropriate, provide physical locks on devices and their communication ports to minimize tampering; and
- Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.

Ensure Trusted Content

- Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification;
- Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer; and
- Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption.

Detect, Respond, Recover

- Technical Protection Measures (security software) on the device that ensure that the security and integrity of the device source code is protected. If the security software is not configured correctly, or if a new vulnerability is discovered in that software, it may be possible to compromise the security software and gain access to the device source code.
- Technical Protection Measures that protect the device from malicious code via regular software updates and/or malware protection software. If new security vulnerabilities are discovered in a particular type of device, and the device software and/or the malware software on the device has not been updated to eliminate the vulnerability, malicious actors could engage in circumvention activities that exploit the vulnerability to inject malicious code into a device, and take control of it.
- Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use;
- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event;
- Implement device features that protect critical functionality, even when the device's cybersecurity has been compromised; and
- Provide methods for retention and recovery of device configuration by an authenticated privileged user.

ITEM 5. ASSERTED NONINFRINGING USE(S)

Alternatives that do not require unauthorized circumvention to study the security of medical devices exist in the form of formalized research agreements that include protections for intellectual property, provide for authorized circumvention activities if needed, and for protection of patient safety, patient privacy and intellectual property.

ITEM 6. ASSERTED ADVERSE EFFECTS

No compelling public interest is served by bypassing established intellectual property protection mechanisms for medical devices. No data has been brought forth which demonstrates or suggests that allowing open access to protected code would in any way enhance safety or efficacy of medical devices. The inability to circumvent TPMs employed

by medical device manufacturers in their device(s) is likely to have no or little adverse effects on the infringing use(s). Those interested or intending to research security concerns alternatively may perform such services without infringement through appropriate legal research mechanisms without the proposed circumvention rule making. Existing regulations require manufacturers to monitor safe use of devices and take corrective action as appropriate.

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. 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 the data.

ITEM 7. STATUTORY FACTORS

The introduction of such an exemption in the U.S. to weaken the protection available to innovative businesses would create a dangerous precedent likely to be followed by other countries that may see weakening of IP protection as potentially advantageous for indigenous industry focused on imitation rather than innovation.