UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

[ ] Check here if multimedia evidence is being provided in connection with this comment

ITEM A. COMMENTER INFORMATION

The Advanced Medical Technology Association (AdvaMed) is a trade association representing the world's leading innovators and manufacturers of medical devices, diagnostic products, digital health technologies, and health information systems. Together, our members manufacture much of the life-enhancing and life-saving health care technology purchased annually in the United States and globally. AdvaMed members range from the largest to the smallest medical technology producers and include hundreds of small companies with fewer than 20 employees. Our members are committed to developing new technologies and services that allow patients to lead longer, healthier, and more productive lives. The devices made by AdvaMed members help patients stay healthier longer and recover more quickly after treatment and enable clinicians to detect disease earlier and treat patients as effectively and efficiently as possible. Strong intellectual property protections, including copyright protection for source code and device outputs, are essential to developing and bringing medical technologies to market.

Christopher L. White
Chief Operating Officer and General Counsel
Advanced Medical Technology Association (AdvaMed)
701 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20004
cwhite@advamed.org
202-783-8700

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 12: Computer Programs—Repair and the proposed expansion to Medical Devices

ITEM C. OVERVIEW

For the reasons stated below, we respectfully request that the Copyright Office oppose the inclusion of medical devices in Proposed Class 12.

Position Summary

- Allowing unauthorized circumvention of Technological Protection Measures (TPMs) in medical devices can harm patients, compromise patient privacy, and place valuable intellectual property at risk.
- Permitting unauthorized circumvention to maintain, repair, or modify a medical device without FDA oversight and without the manufacturer's consultation will endanger patients.
    - AdvaMed is aware of at least 281 adverse events (also referred to as Medical Device Reports or MDRs) from 2012 to 2017 associated with third party servicing. For some devices (e.g., imaging devices), up to 38,500 patients and/or operators were exposed to the potential for harm.
- No exemption should be granted to permit modification of a medical device
    - Under FDA regulations, modifications to a medical device, including changes to service parts and servicing instructions, must be evaluated to determine if the changes trigger a new FDA review or approval for safety and efficacy.
    - Unauthorized Independent Service Organizations (ISOs), which are commercial organizations in the business of providing maintenance and repair services, are not regulated by the FDA. As a result, there is no awareness or oversight if an unauthorized ISO intentionally or unintentionally modifies a medical device during servicing. For example, it was reported that an unauthorized ISO used replacement parts from a hardware store instead of Original Equipment Manufacturer (OEM) verified parts, which are required to be tested for biocompatibility, toxicity, strength, and other specifications essential to the safety and efficacy of the device.
- No exemption should be granted for medical device diagnosis, maintenance, or repair by Unauthorized ISOs.
    - Robust service and repair offerings already exist through OEMs and *authorized* ISOs (third-party service/repair organizations that the OEM authorizes, trains, and ensures has the necessary equipment to perform maintenance and repair services on OEM devices). These entities can ensure that the necessary protections for patient safety, patient privacy, and intellectual property are in place and maintained.

        - These protections include obligations to adhere to FDA Quality System Regulation (QSR) requirements, which include the following (among others):
            - the obligation to develop and preserve proper records regarding servicing of each device;
            - training – including documentation of training – and maintenance of certification for service personnel;
            - calibration of equipment used to repair devices;
            - use of appropriately tested and validated replacement parts;
            - reporting of serious adverse events and injuries to FDA regarding devices they have repaired; and
            - registration of facilities to enable FDA inspection of compliance to these FDA QSR regulations.
    - Unauthorized ISOs have no obligation to follow rigorous QSR requirements.
    - 17 USC 117(c) limitations do not apply to the use of some medical device embedded diagnostic software accessed by unauthorized ISOs through TPM circumvention and utilized to diagnose maintenance and repair issues.
        - This diagnostic software embedded in the medical devices is both (1) not necessary for the activation or routine operation of the device and (2) neither sold/leased nor licensed to the owner/lessee of the medical device.
            - Such embedded diagnostic software is specifically excluded from what is sold, leased, or licensed to the device owner/lessee, and only authorized servicers are permitted to access it.
            - The sales/lease agreements for these medical devices also include provisions that control how and who may service the device.
    - An exemption for medical device diagnosis, maintenance, and repair has the potential to embolden piracy of accessory/add-on functionality, subscription-based functionality, and standalone software on medical devices.
- An exemption that includes medical devices may also negatively impact medical technology innovation, health care costs, and supply chain integrity.

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

The following are examples of the Technical Protection Measures (TPMs) used on medical devices and/or 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

- TPMs 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 gain access to the device improperly.
- 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. Through observation and monitoring of the device through circumvention activities, an 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 or is exposed by circumvention activities, encryption can be bypassed.
- Where appropriate, a layered authorization model is employed 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 preventing the use of a "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, providing 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.

Limit Access to Purchased or Leased Functionality/Services and Prevent Unauthorized Copies

- TPMs, such as a layered authorization model, are used to limit access to only those functionalities or services that were purchased or leased.
    - Additional functionalities, analytics, and integrations are made available for purchase, lease, or subscription and are often provided for, at least in part, by copyrighted software.
    - In some medical devices, the copyrighted software code can perform certain operations on another independent computer (e.g., personal computer with a Unix operating system) that was not purchased or leased with the medical device.
    - Some copyrighted software in medical devices is owned by an entity that is not the medical device manufacturer and is licensed to certain specified entities that do not include the owner/lessee of the device. In some of these instances, the medical device manufacturer is contractually obligated to protect the software code from unauthorized access and copying.
    - TPMs are also used to protect some diagnostic software embedded in medical devices that is both (1) ***not*** necessary for the activation of the device and (2) neither sold/leased nor licensed to the owner/lessee of the medical device. Such diagnostic software is only licensed for access and use by specified authorized servicers.

Ensure Trusted Content

- Restrict software or firmware updates to authenticated code. One authentication method manufacturers may utilize 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

- TPMs (security software) on the device to ensure that the security and integrity of the device source code is protected. If the security software is not configured correctly or a new vulnerability is discovered in that software, it may be possible to compromise the security software and access 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 E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

Whether the proposed class includes at least some works protected by copyright.

1. The Extension of Proposed Class 12 to Cover Computer Programs that are Contained in and Control the Function of Medical Devices Includes At least Some Works Protected by Copyright

While such determinations are fact-specific, copyright protection generally extends to computer programs on medical devices. The source code and object code in a medical device can include protectable original expressions under copyright law.[1] Copyright protection may extend beyond the literal code to the software's structure, sequence, and organization.

Outputs from a medical device can also constitute copyrightable subject matter. While such a determination is also fact-specific, copyright protection in device outputs may extend to, for example, the structure, format, and arrangement of the output data.[2]

[1] See *Apple Comput., Inc. v. Franklin Comput. Corp*., 714 F.2d 1240, 1248-49 (3d Cir. 1983) ("[A] computer program, whether in object code or source code, is a "literary work" and is protected from unauthorized copying, whether from its object or source code version.")

[2] *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).

Whether the uses at issue are noninfringing under title 17.

2. Uses at Issue are Infringing Under Title 17

(a) Fair Use

In determining whether the use made of a copyrighted work in any particular case is a noninfringing fair use, the following four factors are considered: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[3]

(i) The Purpose and Character of the Use is Commercial in Nature

Repairs conducted by a company or a technician engaged in the business of repairing embedded software or software-enabled devices would likely be considered a commercial use.[4] The primary proponents are for-profit Independent Service Organizations (ISOs) who are in the business of providing maintenance and repair services for medical devices. They seek the inclusion of medical devices in Proposed Class 12 to expand their commercial offerings to also include the diagnosis, maintenance, repair, and modification of medical devices without an OEM's authorization. The commercial nature of this use weighs against considering this use to be fair.

Some unauthorized ISOs have circumvented TPMs on medical devices and accessed copyrighted software to utilize software programs that were not sold/leased/licensed to the device's owner/lessee. This includes embedded software that is not necessary for the activation of the device. Examples of such embedded software are programs that diagnose maintenance and repair issues, collect and transmit certain data, perform analytics that are not essential to the device's operation, aid in planning medical treatments, and enhance or reconstruct images.

Similar unauthorized ISOs have circumvented TPMs and cloned the software on a medical device they serviced for one client and copied that software onto another client's devices. In one case, embedded treatment planning software, which is sold as an entitlement and not enabled unless separately purchased, was purchased by one client for a single device. An unauthorized ISO cloned the software in its enabled form and copied it onto 40 devices owned by

[3] 17 U.S.C. §107

[4] U.S. Copyright Office, Software-Enabled Consumer Products 39 (2016), https://www.copyright.gov/policy/software/software-full-report.pdf

unrelated entities that did not purchase the treatment planning software. While this use is outside the scope of Proposed Class 12, there are legitimate concerns that granting the proposed exemption would embolden such acts of piracy.

There is also a commercial benefit to offering maintenance and repair services without authorization. Unauthorized ISOs have fewer costs relative to authorized ISOs who are contractually obligated to undergo OEM approved training, adhere to FDA Quality System Regulation (QSR) requirements, protect patient privacy, and protect intellectual property. Authorized ISOs are provided with a license and an authorized means to access copyright-protected software on medical devices that includes software that is involved in the function of the device (e.g., software to enter settings) and software that is not necessary for the function of the device (e.g., software that diagnoses maintenance and repair issues), which is not sold/leased/licensed to the device owner/lessee.

(ii) Some Copyright Work on Medical Devices is Unpublished in Nature.

The use of unpublished work is less likely to be considered fair. Some copyright protected software on medical devices is not published.

(iii)Diagnosis, Maintenance, Repair, and Modification of Medical Devices Often Involve Using All or Substantial Portions of the Copyrighted Work.

Using all or substantial portions of a copyrighted work weighs against considering this use to be fair.

(iv) Uses at Issue Have the Potential to Harm the Value of the Copyrighted Work

Unlike software-enabled consumer products, there is a market for some medical device software modules as standalone works. Some software on medical devices is activated and maintained through a subscription model. Other software in medical devices can also function on independent, unrelated computers (e.g., a personal computer with a Unix operating system can run certain analytical and image processing software installed in some diagnostic imaging workstations).

In some instances, the medical device manufacturer is not the owner of the copyright of certain software modules integrated into a medical device. For example, some medical devices are developed through a collaboration between a medical device manufacturer and a robotics and software company. In certain instances, some limitations in the software license are due to constraints imposed by a third-party collaborator (in the above example, the robotics and software company that owns the copyright to certain software modules), which are distributed with the device via written licensing

agreements. In such instances, there are contractually obligated limitations specifying that maintenance and repair of certain aspects of the device may only be performed by the third-party robotics and software developer (i.e., the device manufacturer itself may not perform the maintenance or repair on certain aspects of the device).

The use at issue is the diagnosis, maintenance, repair, or modification of a medical device by an ISO that is not authorized by the OEM. Such uses can result in patient injury, compromise patient privacy, and place valuable intellectual property at risk, all of which can harm the value of the copyrighted work. Unauthorized ISOs have no obligation to follow rigorous FDA Quality System Regulation (QSR) requirements. These patient safety concerns are not hypothetical. Please see the section covering the fifth statutory factor below for a more fulsome discussion with examples.

(b) Section 117 Limitations of Exclusive Rights

(i) The section 117(a)(1) limitation on exclusive rights does not apply to a number of medical devices where the owner of the device is not an owner of a copy of one or more software modules that control certain functions of the device.

Section 117(a) only applies to the "owner of a copy of a computer program."[5] The software on numerous medical devices is provided through a written license agreement.

Some software program modules and associated functionalities are activated and maintained through a time-based subscription service. Where software is integrated into a device that is sold, the *Vernor* test can be used to determine whether a transaction should be characterized as a sale or a license. Under *Vernor*, "a software user is a licensee rather than an owner of a copy where the copyright owner: (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions."[6] For some software modules, a nontransferable license is provided, or transfer of the license requires the copyright owner's consent. Such licenses generally prohibit modification, translation, and reverse-engineering and may impose use restrictions. For example, the medical device discussed above in 2(a)(iv) above contractually limits maintenance and repair to the third-party robotics and software company that co-developed the medical device with the manufacturer.

[5] 17 U.S.C. § 117(a)

[6] *Vernor v. Autodesk, Inc.,* 621 F.3d 1102, 1111 (9th Cir. 2010)

Other software embedded in medical devices is not sold/leased/licensed to the owner/lessee of the medical device. This includes software that is not necessary for the operation or function of the device. Examples of this include software that diagnoses maintenance and repair issues, data collection software, and data analytics software, among others.

(ii) The section 117(c) limitation on exclusive rights for maintenance and repair does not apply to the proposed use of modifying a medical device.

One of the uses at issue for Proposed Class 12 is the modification of a medical device. The section 117(c) defense is limited to maintenance and repair as defined in section 117(d). Although the definition includes "any changes to those specifications authorized for that machine," the lessee of a medical device would generally violate a contractual obligation by modifying or authorizing a third party to modify the device without the authorization of the lessor. A similar violation occurs in analogous situations where the software is provided under a written licensing agreement, which generally prohibits modification of the device.

(iii)The section 117(c) limitation on exclusive rights for maintenance and repair does not apply to embedded diagnostics software that is not necessary for the machine to be activated.

Some software embedded in medical devices is not sold/leased/licensed to the owner/lessee of the medical device. This includes software that is not necessary for the activation of the medical device, which is excluded from the limitation on rights for maintenance and repair under 17 USC 117(c)(2). Examples include embedded software that diagnoses maintenance and repair issues, collects data, and performs analytics. Unauthorized ISOs circumvent TPMs to utilize embedded software programs during unauthorized servicing.

3. Users are Not Likely to be Adversely Affected in their Ability to Make Noninfringing Uses.

In assessing the adverse effect, the following five statutory factors in 17 USC §1201(a)(1)(C) must be balanced: (i) The availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (v) such other factors as the Librarian considers appropriate.

(i) The availability for use of copyrighted works is not impacted

Proponents offer that access to copyrighted works is diminished because unauthorized ISOs are deterred due to the prohibition on circumventing TPMs and claim that the situation has worsened because of the pandemic. However, there is no evidence that hospitals are having any difficulty finding properly trained servicers for their devices,

either from the original manufacturer or their authorized repair technicians. These authorized servicers are conducting on-site repairs, providing remote technical assistance, and delivering necessary replacement parts without interruption to patient care. Medical technology companies are successfully working hand-in-glove with hospitals, clinics, and other health care institutions to service, repair, and maintain crucial medical devices. Ultimately, to ensure patient safety, unauthorized ISOs need more than just access to a repair manual to fix and maintain these sophisticated, life-saving medical technologies properly. They need the same knowledge, training, and expertise the OEMs and authorized ISOs have. Even one minor miscalculation could lead to catastrophic injury—to the patient or the device user. Until there is evidence of an actual shortage of properly trained service technicians, the movement to lower medical device repair standards remains a solution in search of a problem. Alternatives that do not require circumvention exist to diagnose, maintain, and repair medical devices. Authorized ISOs have OEM-granted access mechanisms to diagnose, maintain, and repair devices and are a preferred alternative for patient safety. Owner or lessee users of medical devices can also have their staff become authorized to diagnose, maintain, and repair devices through training programs and undertaking certain QSR obligations.

(ii) The availability for use of works for nonprofit archival, preservation, and educational purposes is not especially relevant to the use at issue.

(iii) The impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research is also not particularly relevant to the use at issue.

(iv) The circumvention of technological measures has the potential to affect the value of copyrighted works negatively.

The circumvention of access controls on medical devices could result in a diminution in the value of copyrighted works if those medical devices could no longer reliably protect the computer programs, patient data, and analytics operating on and produced by the medical devices. There are also concerns about accessing and activating software modules that are purchased or licensed separately following an additional purchase or subscription model. Activating such software modules without authorization would obviously negatively affect the value of that copyrighted work.

(v) Such other factors as the Librarian considers appropriate.

Patient safety should be the highest priority concern and substantially outweigh other factors. Medical device manufacturers are highly regulated to ensure that devices continue to be safe and effective for patients for their intended use. OEMs are required by regulation to qualify or validate service instructions and parts for new medical devices to ensure there is no impact on the safety and effectiveness of their devices during OEM servicing. Additionally, by regulation, design changes to a medical device, including changes to service parts and servicing instructions, must be

evaluated to determine if the changes trigger a new FDA review or approval before they can be implemented.

ISOs are not regulated by the FDA. As a result, there is no awareness or oversight if an unauthorized ISO intentionally or unintentionally modifies a device during servicing. For example, in one instance, an unauthorized ISO used replacement parts from a hardware store instead of the OEM verified parts, which are required to be tested for biocompatibility, toxicity, strength, etc. The result is that unauthorized ISO serviced devices may no longer be as safe and effective as the original device, with the potential for serious patient or user injuries.

In contrast, OEMs are required by regulation to qualify or validate service instructions and parts for new medical devices to ensure there is no impact on the safety and effectiveness of their devices during OEM servicing. Additionally, OEMs must follow other regulatory requirements, including those from the FDA Quality System Regulation (QSR), which require the following (among others):

- the development and preservation of proper records regarding servicing of each medical device;
- training – including documentation of training – and maintenance of certification for service personnel;
- calibration of equipment used to repair devices;
- use of appropriately tested and validated replacement parts;
- reporting of serious adverse events and injuries to FDA regarding devices they have repaired; and
- registration of facilities to enable FDA inspection of compliance to FDA regulations.

Under the QSR, OEMs are required to update and maintain strict revision control on servicing documentation and device software, and to ensure that their trained and authorized service representatives are utilizing the most up-to-date information. OEMs are also required to audit their service representatives to ensure they are using appropriate servicing documentation for the model of the device they are servicing. Failure to do so could have serious implications for patient safety.

ISOs authorized by OEM are contractually obligated to implement these requirements.

These patient safety concerns are not hypothetical. AdvaMed is aware of at least 281 adverse events (also referred to as Medical Device Reports or MDRs) from 2012 to 2017 associated with third party servicing. For some devices (e.g., imaging devices), up to 38,500 patients and/or operators were exposed to the potential for harm.

Actual or potential patient and/or operator impacts from these reports include:

- Screwdriver tip lodged in a patient;
- Operator injury, counterpoise support system arm (80-93 pounds) struck operator;
- Potential for repeat CT scans and contrast administration with the concomitant risk of additional radiation exposure;
- Potential for burns including internal or oral 3rd-degree burns, which may not be apparent until burning tissue is sensed;
- Delayed surgery (potential for worsening patient condition);
- Prolonged surgery (may result in longer exposure to anesthesia, a greater potential for infection, and more blood loss);
- Potential for concussions and/or fractures;
- Infusion therapy - Air in System – potential harms include death, neurological changes, stroke, seizures, cardiac and/or respiratory arrest, pain, decreased oxygenation, arrhythmia, pulmonary hypertension;
- Delays in infusion therapy with the delay of pharmacological effects and/or worsening of condition including death;
- Insufficient or excessive infusion therapy or interruption of therapy and/or worsening of condition including death; and
- Temporary hearing loss; ringing in ears.
- Below are examples of unauthorized ISO “servicing” (which should actually be deemed remanufacturing under FDA regulations).

Figure 1. The angle cover on an endoscope was replaced with a material resembling plastic wrap.

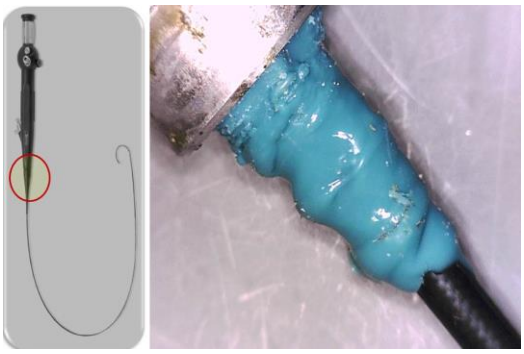

Figure 2. The shaft adapter on an endoscope was repaired using a putty-like material of questionable provenance.

In these examples, unauthorized ISOs clearly used components that are not likely biocompatible and likely would not withstand the reprocessing and sterilization process. It is also likely that these repairs, particularly Figure 1, compromised the device's ability to perform its key function of accessing a patient's anatomy.

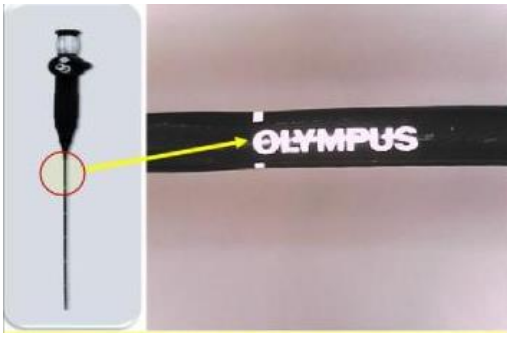

Figure 3. An Olympus component was inserted into a KARL STORZ endoscope shaft.

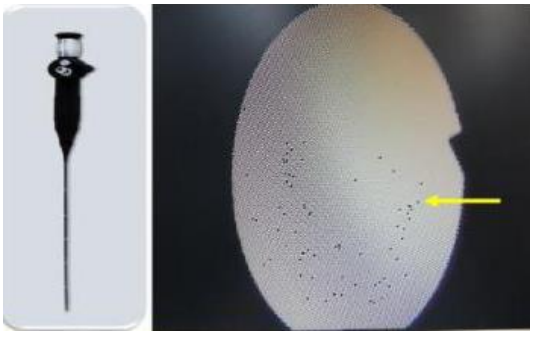

Figure 4. Broken image fibers in an endoscope.

Examples in Figure 3 and Figure 4 are equally if not more concerning than the previous examples because they show that a device can be modified such that the physician or patient cannot see the change.

Granting an exemption to allow circumventing TPMs to diagnose, maintain, or repair medical devices also raises concerns about whether the TPMs will be safely restored. Critical design details and software code could be accessed more easily by entities with malicious intent who could use the information to develop counterfeit devices, counterfeit software (for the software modules that stand alone), or who could intentionally modify devices in order to harm patients. Lastly, if an exception is granted for medical devices, there may be a negative impact on medical technology innovation, health care costs, and supply chain integrity.