

Before the United States Copyright Office and Library of Congress
In the Matter of Exemptions to Permit Circumvention of Access Controls on Copyrighted Works
Docket No. 2026-4 | Tenth Triennial Section 1201 Rulemaking (2027 Cycle)

Comments of the Advanced Medical Technology Association (AdvaMed) in Opposition to the Petition to Expansion the Medical Device Repair Exemption

Interested Party:

Advanced Medical Technology Association (AdvaMed), the Medtech Association, appreciates the opportunity to provide comments and evidence in opposition to the proposed expansion of the exemption at 37 C.F.R. § 201.40(b)(17). AdvaMed is the leading trade association of the medical technology industry, representing more than 650 companies that develop, manufacture, and distribute medical devices, diagnostic tests, digital health technologies, and medical imaging products. AdvaMed's membership spans the entire medical technology sector, including small, entrepreneurial innovators, mid-sized companies, and global industry leaders, giving the Association a uniquely comprehensive perspective on the opportunities and challenges facing medtech companies of all sizes.

AdvaMed is uniquely positioned to provide a comprehensive industry perspective on issues affecting the development, regulation, and availability of medical technologies. AdvaMed advocates for innovative technologies that save and improve lives, enable earlier diagnosis and treatment, enhance quality of life, and help create a more efficient and sustainable health care system.

Contact Information:

Peter Weems
Senior Vice President, Digital & Diagnostic Technologies
Advanced Medical Technology Association (AdvaMed)
1301 Pennsylvania Avenue, NW, Suite 400, Washington, DC 20004
pweems@advamed.org

Terry Chang, M.D., J.D.
Vice President, Assistant General Counsel, and Director, Legal & Medical Affairs
Advanced Medical Technology Association (AdvaMed)
1301 Pennsylvania Avenue, NW, Suite 400, Washington, DC 20004
tchang@advamed.org

Subjects of This Submission

This submission addresses the proposed expansion of the current medical device repair exemption codified at 37 C.F.R. § 201.40(b)(17): “Computer programs that are contained in and control the functioning of a lawfully acquired medical device or system, and related data files, when circumvention is a necessary step to allow the diagnosis, maintenance, or repair of such a device or system.”

- An expansion is sought by Marshall R. Shannon in the submission docketed at COLC-2026-0100-0006 and captioned “Petition to Renew and Supporting Statement and Petition for a New or Modified Exemption for Medical-Device Diagnosis, **Installation**, Maintenance, Repair, **Calibration**, and **Return to Service**.” That submission combines a request to renew § 201.40(b)(17) as written with a request for a materially broader exemption. These comments address only the second request.
- Another expansion is sought by TriMedx Holdings, LLC (COLC-2026-0100-0044) asks the Office to “continue and renew the exemption under 17 U.S.C. § 1201(a)(1) that allows circumvention of technological measures applied to software programs and data files in medical devices for the purpose of diagnosis, maintenance, repair, and regulatory compliance of such devices”, adding “**regulatory compliance**” to the class defined in 37 C.F.R. § 201.40(b)(17).

AdvaMed files this submission separately because the Office has instructed that “[e]ach submission must address only a single exemption,” while “participants may submit multiple comments to address multiple exemptions.” The expansion Mr. Shannon proposes is, by the Office’s own definition, not the current exemption: petitions for new exemptions “cover activities not currently permitted by any existing exemption, including those that would expand the scope of a current exemption.” AdvaMed’s opposition to renewal of § 201.40(b)(17) as currently written is submitted concurrently and separately, in its Comments in Opposition to Petitions to Renew the Medical Device Repair Exemption. The two submissions are complementary, and the evidence filed as Exhibits A through D accompanies both.

I. INTRODUCTION AND SUMMARY OF OPPOSITION

AdvaMed opposes the proposed expansion for two independent sets of reasons — one procedural, one substantive — and asks the Office to give the expansion no effect in this phase.

The procedural objection is straightforward. The Office’s notice of inquiry permits a renewal petition to seek readoption of a current exemption “as currently written in the Code of Federal Regulations, without modification,” and provides that “a petitioner may not use a renewal petition to request new language or exempted activities for a current exemption.” Mr. Shannon filed his expansion request in his petition to renew. The Office states that Mr. Shannon’s petition is being considered as a renewal

petition.¹ Under the Office’s rule, that submission “shall be considered solely as a renewal petition,”² and the expansion drops out of this phase entirely. However, the Office also appears to consider the same submission as a new petition,³ as the Office may nonetheless decide to carry some part of the request forward as a new petition.

The proposal, if adopted, would resolve against AdvaMed’s members the precise question the D.C. Circuit held had never been litigated on any record. Four features of the proposal are disqualifying. It defines a class that begins with programs that “operate” and “control” medical devices and ends with “technical materials” generally, collapsing into one class the clinical operation software and the Servicing Works that the court’s reasoning depends on keeping apart. It reaches activities — installation of resold systems, commissioning, cybersecurity reconfiguration — that the exemption’s own definitions of “maintenance” and “repair” exclude. It asks for authority over “certificates” and “credentials,” which on this record are not works behind the access control but the access control itself. And a substantial part of it asks the Librarian for presumptions, safe harbors, and fee-shifting — relief § 1201(a)(1)(C) does not authorize anyone to grant.

AdvaMed accordingly asks the Office to give the expansion no effect in this phase; in the alternative, if any portion is carried forward as a petition for a new exemption, to organize it as a separate proposed class in the notice of proposed rulemaking and to solicit a full record on it. AdvaMed reserves its complete legal and evidentiary case for the public comment phase, where the Office has directed that such records be built.

Defined terms used here follow AdvaMed’s companion renewal comment. Clinical Operation Software is the software health care professionals use to operate a medical device to perform patient care activities. System Servicing / Diagnostic Software and Maintenance-Related Documentation are referred to collectively as Servicing Works.

Clinical Operation Software is the software that HCPs use to operate a medical device to perform patient care activities.

System Servicing/Diagnostic Software includes software applications, diagnostic tools, calibration programs, configuration utilities, service interfaces, and related digital resources used to install, inspect, calibrate, test, maintain, diagnose the system, troubleshoot, update, or repair a medical device to its intended performance and safety specifications. For example, System Servicing/Diagnostic Software can be used to:

¹ Section 1201: *Petitions to Renew Prior Exemptions*, U.S. Copyright Off., <https://www.copyright.gov/1201/2027/petitions/renewal/> (last visited Sept. 22, 2026) (noting that the Office elected to treat Shannon’s submission as a renewal petition).

² 91 Fed. Reg. 34797

³ Comment COLC-2026-0100-0060, Regulations.gov, <https://www.regulations.gov/comment/COLC-2026-0100-0060> (last visited Sept. 22, 2026) (Displaying the identical submission as, “New Petition – Marshall Shannon”).



- Check for system errors or malfunctions;
- Access system diagnostic information and service logs;
- Calibrate the device after a repair;
- Troubleshoot errors;
- Install software updates or patches; and/or
- Verify that the device is functioning properly before it returns to clinical operation use for patients.

Maintenance-Related Documentation is non-software, digital work used for servicing, such as digital service manuals or repair procedure documentation.

Servicing Works refers to System Servicing/Diagnostic Software and Maintenance-Related Documentation, collectively.

II. FIRST EXPANSION REQUEST

A. What the petition proposes

Mr. Shannon asks for two things. He “requests renewal of the existing exemption for circumvention of technological protection measures on lawfully acquired medical-device software when necessary for diagnosis, maintenance, or repair.” He then separately requests “clarification or a modified exemption expressly covering owner-authorized installation, reinstallation, software setup, operating-system and application restoration, relocation, commissioning, calibration, performance verification, service-data access, cybersecurity-related reconfiguration, and return to service for new, used, and resold medical devices.”

The class he proposes reads in full:

Computer programs that operate, control, diagnose, monitor, configure, calibrate, install, service, maintain, test, or restore medical devices or systems, including related service interfaces, logs, configuration data, certificates, credentials, utilities, and technical materials, when circumvention is performed by the owner or an authorized service provider solely for lawful diagnosis, installation, maintenance, repair, calibration, cybersecurity, or return to service.

B. Why AdvaMed addresses some of the substance now, and what it reserves

Although this “is not the phase for full legal and evidentiary submissions on proposals for new exemptions, which will be solicited during the public comment phase,”⁴ several features of the proposal raise threshold questions of authority rather than questions of evidence. The Register “will

⁴ 91 Fed. Reg. 34796

not at this phase reject any petitioned-for exemption unless it fails to meet the threshold requirements of section 1201(a),” and AdvaMed submits that parts of this proposal do not meet them.

AdvaMed expressly reserves the remainder of its case. If any portion of the proposed expansion is carried forward into the public comment phase, AdvaMed will submit its complete legal and evidentiary opposition in the round the Office designates for that purpose, and nothing omitted here should be treated as conceded.

C. Proposal Runs Against the Boundary of the Librarian’s Authority

1. Credentials and certificates are the access control, not a class of works behind it

The triennial rulemaking, as the notice of inquiry states, “addresses only the prohibition on circumvention of access controls; the statute does not grant authority to adopt exemptions to the anti-trafficking provisions of sections 1201(a)(2) or 1201(b).” The proposed class expressly includes “certificates, credentials,” and the petition asks that covered circumvention encompass the “creation, modification, replacement, renaming, movement, reset, restoration, or deletion of files, registry entries, certificates, credentials, settings, scheduled tasks, or network destinations.”

On the evidence AdvaMed submits with these comments, those artifacts are not works sitting behind a technological measure. They are the measure.

Exhibit	The artifact that constitutes the technological protection measure
Exhibit A [Carestream]	The “SecureLink” credential — a USB multifactor-authentication device containing an encrypted file identifying the individual service engineer, used with a password unique to that engineer.
Exhibit C [Philips]	The encrypted, user-specific certificate presented by a physical smartcard through the Integrated Security Tool, together with the matching account password; the certificate is valid only on the user’s registered computer.
Exhibit D [Siemens Healthineers]	The service key — a character string, generally 256 characters, generated from information specific to the device or supplied by a USB dongle, time-limited and tiered, and distributed and approved by the manufacturer.

A rule permitting these to be created, replaced, reset, or restored at will would not be an exemption from the prohibition on circumventing an access control. It would be authorization to manufacture the key. The distinction matters under the statute: § 1201(a)(1)(C) empowers the Librarian to exempt classes of works from the access-control prohibition, not to bless the fabrication or substitution of the credentials that implement it, and § 1201(a)(1)(E) confirms that a determination in this proceeding may not be used as a defense to a claim under § 1201(a)(2) or § 1201(b). A class drawn to include credentials and certificates invites exactly the confusion those provisions were written to prevent.

2. A class defined by the petitioner’s purpose is not a class of works



The proposed class is also defined in substantial part by who is circumventing and why — it applies “when circumvention is performed by the owner or an authorized service provider solely for lawful diagnosis, installation, maintenance, repair, calibration, cybersecurity, or return to service.” The statute directs the Librarian to determine whether users are adversely affected “in their ability to make noninfringing uses under this title of a particular class of copyrighted works.” The class is of works. Purpose-based and user-based conditions have a place as limitations on an exemption, and the current exemption contains them; they cannot do the work of identifying the works themselves. Here they are asked to, because the work-side of the definition has been drawn so broadly that nothing else constrains it.

3. The Remote-Monitoring and Data-Pathway Request Falls Outside This Proceeding

The petition asks that an owner or authorized service provider “be permitted to disable, block, reconfigure, or remove remote monitoring, automatic uploads, SMTP destinations, credentials, certificates, scheduled tasks, and related pathways for cybersecurity, privacy, service transition, or data-governance reasons.” The pathways it describes carry “status notifications, error logs, utilization information, service events, and related data.”

Whether such a pathway may be disabled, and by whom, is not a question about access to a copyrighted work. Disabling a manufacturer’s remote monitoring does not give anyone access to a work; it stops the flow of device-generated data. The request therefore falls outside the adverse-effect inquiry § 1201(a)(1)(C) assigns to the Librarian, which asks whether the anticircumvention prohibition impairs the ability to make noninfringing uses of copyrighted works.

The request also reaches subject matter committed to other regimes. Remote monitoring pathways support device performance monitoring, cybersecurity patching, and a manufacturer’s continuing obligations with respect to devices it has placed into service, including postmarket surveillance. No record in this proceeding addresses what would follow from authorizing their removal, and the Office is not the body to build one. AdvaMed asks the Office to decline to reach the request.

4. The “Commingling” Theory Asks for a Rule of Decision, Not a Class of Works

A substantial portion of the petition asks the Office to adopt principles governing liability rather than to define a class of works. It asks the Office to “separate access from use”; to hold that “[e]ntering a combined service environment should not create an irrebuttable presumption that the servicer opened, copied, or used every protected work available within that environment”; to direct that a manufacturer-prescribed software reload “should not, by itself, support an inference of evidence destruction”; to convene “a formal stakeholder meeting, technical conference, roundtable, evidentiary hearing, or other proceeding”; and to preserve a record for congressional review of whether “additional statutory protections, fee-shifting, a safe harbor, an enforcement mechanism, or formal coordination are needed.”



Section 1201(a)(1)(C) directs a prospective, class-based determination about the succeeding three-year period. It does not authorize the Librarian to allocate burdens of proof, to create or foreclose presumptions about what a litigant accessed, to establish safe harbors, or to shift fees. Those are matters for Congress and for the courts in which such questions arise. An exemption is a definition of what may be circumvented; it is not a rule of decision for disputes about what a servicer did after circumventing.

The Office has said plainly that the streamlined proceeding “is not a forum to litigate other concerns,” and that comments should not address “whether any user’s activities may or may not be consistent with the exemption” as codified. That constraint binds proponents as much as opponents. AdvaMed accordingly does not respond to the characterizations of particular disputes set out in the petition, takes no position here on any of them, and asks the Office not to rest any determination on them.

The petition is also closely bound up with its author’s own litigation. AdvaMed notes that a triennial exemption is not a vehicle for revisiting an adjudicated dispute, and that an exemption to § 1201(a)(1) would not in any event answer the contract, trade secret, and computer-access claims the petition describes.

D. The Expansion Petition’s Own Account Supports AdvaMed on the Dispositive Fact

One part of the petition deserves the Office’s particular attention, because it is the most detailed account in this docket of how the works at issue are actually controlled — and it comes from the petitioner.

Mr. Shannon contends that a Philips service pack “would thereafter be required to access on device software tools,” that a user “would need a Philips IST smartcard, a valid IST account, and the appropriate system entitlements”; that customer biomedical engineers received “only a restricted set of service documentation and software tools”; that certain tasks were “placed at Level 2 for Philips field service engineers and authorized trade partners”; and that service manuals were reclassified from one CSIP level to another. He describes “a mapping among CSIP level, IST entitlement, and the service level recognized by the software,” and objects that “a user may therefore confront one technological gate controlling multiple layers of service functionality.”

His objection is to that architecture. But his description of it is evidence, and it corroborates the manufacturer declarations on every material point: the Servicing Works sit behind a manufacturer-administered technological measure distinct from the measures that control access to Clinical Operation Software; access is granted by entitlement level; and the levels are tied to training, authorization, and contractual status. That is a separately controlled, separately licensed body of works. It is the proposition the D.C. Circuit held had never been established, offered here by a proponent of the exemption — and it is the reason a class that merges those works with Clinical Operation Software should not be adopted without a record.



III. SECOND EXPANSION REQUEST: THE “REGULATORY COMPLIANCE” PURPOSE SOUGHT BY TRIMEDX

TriMedx Holdings, LLC (COLC-2026-0100-0044) asks the Office to “continue and renew the exemption under 17 U.S.C. § 1201(a)(1) that allows circumvention of technological measures applied to software programs and data files in medical devices for the purpose of diagnosis, maintenance, repair, and regulatory compliance of such devices”, adding “regulatory compliance” to the class defined in 37 C.F.R. § 201.40(b)(17).

The codified exemption contains no regulatory compliance purpose. It permits circumvention that is “a necessary step to allow the diagnosis, maintenance, or repair” of a device, and § 201.40(b)(17)(i)–(ii) confine maintenance and repair to servicing or restoring a device so that it works in accordance with its original specifications. Regulatory compliance is a broader and differently bounded concept, and the petition illustrates the difference: the incident it recounts concerned access to software keys it contends were needed “to perform assembly, installation, adjustment, and testing (AIAT) procedures on a medical device, as mandated under 21 CFR 1020.30” — assembly and installation activities of the same kind the Shannon petition asks the Office to add.

The Office’s rule resolves it simply: a renewal petition that describes activities broader than the exemption authorizes “shall be considered solely as a renewal petition” for the exemption as written. In the alternative, if any portion is carried forward as a petition for a new exemption, the Office must organize it as a separate proposed class in the notice of proposed rulemaking and solicit a full record on it. AdvaMed reserves its complete legal and evidentiary case for the public comment phase, where the Office has directed that such records be built.

IV. RELIEF REQUESTED

For the reasons set out above, AdvaMed respectfully requests that the Office take the following actions.

First, consider the submission of Marshall R. Shannon (COLC-2026-0100-0006) solely as a petition to renew 37 C.F.R. § 201.40(b)(17) as currently written, and give no effect in this proceeding to the expansion requested within it, consistent with the Office’s instruction that a renewal petition containing such requests “shall be considered solely as a renewal petition.”

Second, decline to adopt the proposed class in any form. It merges Clinical Operation Software with Servicing Works, abandons the containment and control limits of the current exemption, extends to “technical materials” without boundary, and reaches activities the exemption’s own definitions of maintenance and repair exclude.

Third, decline on threshold grounds to reach the portions of the petition that seek authority § 1201(a)(1)(C) does not confer: the treatment of certificates and credentials as works subject to creation, replacement, or reset; the disabling of remote monitoring and automatic data transmission



pathways; and the requests for presumptions, safe harbors, fee-shifting, and enforcement mechanisms.

Fourth, in the alternative, if the Office carries any portion of the expansion forward as a petition for a new exemption, organize it in the notice of proposed rulemaking as a proposed class separate from the renewal of § 201.40(b)(17), state the legal and factual issues on which it seeks comment, and afford opponents the full comment rounds the notice of inquiry provides. AdvaMed will submit its complete legal and evidentiary opposition in that phase.

Fifth, to the extent the TriMedx petition is considered a petition to expand the exemption to also include a “regulatory compliance” purpose the codified exemption does not contain, treat that request the same way and give it no effect in this phase.

Sixth, if the Office reaches the classification question in connection with any expansion, identify for comment the questions AdvaMed has framed in its companion renewal submission: how Servicing Works should be classified relative to Clinical Operation Software; whether the technological measures controlling Servicing Works are separate access controls on a separate class of works; the existence, structure, and economics of the market in which access to Servicing Works is licensed; the significance of hosting Servicing Works off the lawfully acquired device on manufacturer-controlled infrastructure; and the fair-use consequences of each under *Andy Warhol Foundation for the Visual Arts v. Goldsmith*.

V. EVIDENCE SUBMITTED WITH THESE COMMENTS

AdvaMed submits the declarations in Exhibits A-E, each made on the declarant’s personal knowledge by an individual with operational responsibility for servicing the declarant company’s medical devices. The same exhibits accompany AdvaMed’s companion comments opposing renewal, and the exhibit lettering is common to both submissions.

Exhibit	Description	Subject
Exhibit A	Declaration of Garrett Huntley, Senior Director of Federal and Service Solutions, Carestream Health, Inc.	Service and diagnostic applications; SecureLink multifactor service credentials; Service Portal documentation; per-person, per-unit annual subscriptions for third-party service personnel who successfully complete OEM training.
Exhibit B	Declaration of Jerome Duhamel, Global Service Operations GM of GE Medical Systems SCS (an affiliate of “ GE HealthCare ”)	Service and diagnostic applications; Secure Service Access keys (SSA keys): USB key with a Digi code (SSA hard keys) & remotely installed (SSA license keys); Tiered licensing of service software and documentation.



Exhibit	Description	Subject
Exhibit C	Declaration of Pierre Malboeuf, Vice President, Service Delivery, Hologic Inc.	System Servicing/Diagnostic Software licensed to third-party servicing personnel who undergo factory training
Exhibit D	Declaration of Jacqueline Dickson, CSIP Services Operations Director, Philips	Tiered service software and documentation; Integrated Security Tool certificates, smartcards, and entitlements; licensing of Level 1 access under cooperative service agreements; cloud storage of service documentation
Exhibit E	Declaration of Goncalo Arnaut, Head of Customer Services for North America, Siemens Healthineers	System servicing and diagnostic software; service keys and dongles; separate clinical operator logins; leasing and licensing of service access to owners and servicing organizations; cloud hosting

Respectfully submitted,

Advanced Medical Technology Association

/s/

Christopher White
General Counsel and Chief Policy Officer
Advanced Medical Technology Association (AdvaMed)

/s/

Peter Weems
Senior Vice President, Digital & Diagnostic Technologies
Advanced Medical Technology Association (AdvaMed)

/s/

Terry Chang, M.D., J.D.
Vice President, Assistant General Counsel, and Director, Legal & Medical Affairs
Advanced Medical Technology Association (AdvaMed)

September 28, 2026



EXHIBIT A

Declaration submitted in support of Comments from:

Advanced Medical Technology Association (AdvaMed)

1301 Pennsylvania Ave NW, Ste 400

Washington, DC 20004

DECLARATION OF GARRETT HUNTLEY

I, Garrett Huntley, declare as follows based on my personal knowledge:

I. DECLARANT AND COMPANY BACKGROUND

1. I am the Senior Director of Federal and Service Solutions for Carestream Health, Inc. ("Carestream"). I have held this position since 2024. My responsibilities include sale and revenue generation for Carestream's break/fix service business, biomedical and clinical applications training offerings .

2. I have 10 years of experience in contract management, medical imaging equipment sales, and medical imaging equipment service and support. In my role, I am familiar with Carestream's medical devices, clinical operation software, system servicing and diagnostic software, Maintenance-Related Documentation, access controls, licensing practices, and service offerings described below.

3. Carestream develops, manufactures, sells, and/or leases Digital radiography equipment and systems, and associated detectors and generators, along with other medical imaging equipment, used for general clinical purposes, including diagnostic imaging in patient care.

II. RELEVANT SOFTWARE AND MATERIALS

4. As used in this declaration:

- (a) "Clinical Operation Software" means software that health care professionals use to operate a medical device to perform patient care activities;
- (b) "System Servicing/Diagnostic Software" includes software applications, diagnostic tools, calibration programs, configuration utilities, service interfaces, and related digital resources used to install, inspect, calibrate, test, maintain, diagnose, troubleshoot, update, or repair a medical device to its intended performance and safety specifications; and
- (c) Maintenance-Related Documentation is non-software, digital work used for servicing, such as digital service manuals or repair procedure documentation.

5. Carestream uses Clinical Operation Software on its DRX line of X-ray imaging solutions to enable clinicians to acquire, review, and manage diagnostic images and operate the imaging system for patient care. That software includes the Carestream Main Application.
6. Carestream uses System Servicing/Diagnostic Software for those devices. Some of that service and diagnostic software is integrated with the Carestream Main Application, and other service and diagnostic software is managed as standalone applications, such as detector and generator configuration and diagnostic applications. This software is used to check for system errors or malfunctions, access system diagnostic information and service logs, calibrate the device after a repair, troubleshoot errors, install software updates or patches, and verify that the device is functioning properly before it is returned to clinical use.

III. TECHNOLOGICAL PROTECTION MEASURES (TPMs) & DIFFERENTIAL ACCESS

7. Access to Carestream's System Servicing/Diagnostic Software is controlled by a technological protection measure that Carestream refers to as "SecureLink." Access to the service and diagnostic applications requires both a service multi-factor authentication (MFA) device and a password that are unique to each individual service engineer. The USB MFA device contains an encrypted file identifying the service engineer.
8. These TPMs are separate and apart from the protections or controls governing access to the Clinical Operation Software. Carestream service access is unique to Carestream-issued service credentials and the SecureLink MFA device, while clinical users access the Clinical Operation Software using Windows authentication, with optional proximity badge multi-factor authentication.
9. Access to the Clinical Operation Software is controlled by Windows authentication and optional proximity badge MFA, which is administered by the healthcare facility that owns or leases the device and its information technology personnel. By contrast, access to the System Servicing/Diagnostic Software is controlled by the SecureLink service key and the unique service engineer password associated with it, which are issued and administered by Carestream.
10. A person who has authorized access to the Clinical Operation Software does not thereby receive authorized access to the System Servicing/Diagnostic Software. To obtain such access, the person or organization must complete Carestream OEM service training and obtain SecureLink credentials from Carestream, either under an OEM service agreement with Carestream or, in the case of service providers that do not hold a Carestream service agreement, by sending individual field engineers to Carestream OEM service training and paying an annual subscription assessed on a per-person, per-unit basis.
11. These access controls serve to maintain patient safety, cybersecurity control, device integrity, and protect proprietary materials.

IV. LICENSING, SERVICE OFFERINGS, AND DISTINCT MARKET

12. The System Servicing/Diagnostic Software resides on the medical device and is not sold as a standalone product. Carestream provides *access* to this software separately from the sale or lease of the device, through the SecureLink service key and through Carestream's Service Portal. Service Portal and SecureLink access is provided to OEM-trained device owners, channel partners, independent service organizations (ISOs) and multi-vendor service (MVS) personnel contracted to service Carestream equipment.

13. This access to the software is offered both through OEM service agreements and through licensing. Customers who purchase OEM service agreements and who are OEM-trained on the equipment have access via Carestream's SecureLink service key. Other service providers that do not have service agreements with Carestream but service or maintain Carestream equipment, including ISOs and MVS organizations, may send individual field engineers to Carestream OEM service training and pay a yearly subscription on a per-person, per-unit basis to obtain these credentials. The access provided includes the SecureLink service key and credentials, and access to the Service Portal and its Maintenance-Related Documentation described below.

14. The market for these products and services includes biomedical engineers, channel partners, and ISO and MVS field engineers. Carestream competes in servicing and repairing medical devices, including its own, primarily with the third-party service providers, in the form of ISOs and MVS organizations, including MVS organizations operating within competing equipment OEMs such as GE, Philips, and Siemens (Block).

15. Customers can only be assured they are receiving quality maintenance and repair services on their System Servicing/Diagnostic Software if their service personnel have completed Carestream OEM service training and acquired SecureLink credentials and Service Portal access.

V. MAINTENANCE-RELATED DOCUMENTATION

16. Carestream provides extensive Maintenance-Related Documentation to OEM-trained field service engineers. It includes maintenance documentation; service bulletins; software and firmware update information; modification and installation instructions; service documentation, in the form of process checklists, manuals, diagnostic guides, and parts lists; user guides, best practices information, new version release notes; and acceptance and compliance test procedures.

17. This documentation is provided through a web-based portal called the "Service Portal", along with a thumb drive option. It is therefore maintained separately from the Clinical Operation Software and the System Servicing/Diagnostic Software that resides on the device and is accessed through a Carestream-hosted portal rather than through the device's clinical interface.

18. The documentation in the Service Portal is used by OEM-trained field service professionals who maintain SecureLink credentials. They may access the portal at any time, and the portal can

be used to download information or for real time assistance during service, installation, or preventive maintenance activities. The Service Portal provides the same level of detail to outside OEM-trained field service engineers as is supplied to Carestream OEM field engineers.

19. Access to this documentation is controlled by TPMs: the Carestream Service Portal is password protected, and the SecureLink service key requires password authentication. These measures are separate and apart from the protections governing the Clinical Operation Software because Service Portal and SecureLink credentials are issued and controlled by Carestream and are conditioned on completion of Carestream OEM service training. Access to the Clinical Operation Software is controlled by Windows authentication and optional proximity badge MFA administered by the healthcare facility.

VI. UNAUTHORIZED ACCESS [AND PRACTICAL EFFECTS]

20. Carestream developed SecureLink in-house to protect against unauthorized use of, or infringement relating to, its equipment and service resources. Enforcement is contractual, based on agreements with customers and trained service providers who receive the SecureLink passwords after completion of Carestream certified training.

21. Unauthorized circumvention of the TPMs described above would permit persons who have not completed the proper Carestream OEM service training, and who are not subject to the contractual terms under which SecureLink credentials and Service Portal access are granted, to access the System Servicing/Diagnostic Software and Maintenance-Related Documentation, putting patient safety at risk.

VII. CONCLUSION

23. The Clinical Operation Software, System Servicing/Diagnostic Software, and Maintenance-Related Documentation described above are distinct in function and subject to distinct access controls: the Clinical Operation Software is protected by Windows authentication and optional proximity badge MFA administered by the healthcare facility, while the System Servicing/Diagnostic Software and Maintenance-Related Documentation are protected by the SecureLink MFA device, unique service engineer passwords, and by password-protected Service Portal credentials, issued and administered by Carestream.

24. The System Servicing/Diagnostic Software and Maintenance-Related Documentation are monetized through OEM service agreements and through annual per-person, per-unit subscriptions paid by service providers that complete Carestream OEM service training.

25. Allowing improperly trained service personnel to service and repair sophisticated diagnostic equipment is a patient safety risk.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on September 25, 2026, in Rochester, New York.

Garrett Huntley Digitally signed by Garrett Huntley
Date: 2026.09.25 15:29:38 -04'00'

Garrett Huntley
Senior Director of Federal and Service Solutions
Carestream Health, Inc.

EXHIBIT B

Declaration submitted in support of Comments from:
Advanced Medical Technology Association (AdvaMed)
1301 Pennsylvania Ave NW, Ste 400
Washington, DC 20004

DECLARATION OF JEROME DUHAMEL

I, Jerome Duhamel, declares as follows based on my personal knowledge:

I. DECLARANT AND COMPANY BACKGROUND

1. I am the Global Service Operations GM of GE Medical Systems SCS (an affiliate of “GE HealthCare”). I lead our global service operations Center of Excellence across service delivery, commercial enablement, digital platforms, business operations, business intelligence and service productivity.
2. I have 20 years of experience in GE HealthCare product service. In my role, I am familiar with the company’s medical devices, Clinical Operation Software, System Servicing/Diagnostic Software, Maintenance-Related Documentation, access controls, licensing practices, and service offerings described below.
3. GE HealthCare develops, manufactures, sells, and/or leases imaging devices in MR, PET, CT, MI, Xray, and Ultrasound used for diagnostic and interventional procedures.

II. RELEVANT SOFTWARE AND MATERIALS

As used in this declaration:

- (a) “Clinical Operation Software” means software that health care professionals use to operate a medical device to perform patient care activities;
 - (b) “System Servicing/Diagnostic Software” includes software applications, diagnostic tools, calibration programs, configuration utilities, service interfaces, and related digital resources used to install, inspect, calibrate, test, maintain, diagnose, troubleshoot, update, or repair a medical device to its intended performance and safety specifications; and
 - (c) “Maintenance-Related Documentation” is documentation used for servicing, such as service manuals or repair procedures.
4. GE HealthCare uses Clinical Operation Software on all products to enable clinicians to operate the device.

5. GE HealthCare uses System Servicing/Diagnostic Software for above mentioned devices, including Common Service Desktop. This software is used to view logs, test, calibrate, configure, troubleshoot, update or verify performance of the device.

III. TECHNOLOGICAL PROTECTION MEASURES (TPMs) AND DIFFERENTIAL ACCESS

6. Access to the System Servicing/Diagnostic Software is available on the device with no access restriction for all logged users for Class A1 tools (referred to externally as General Service) and controlled by Secure Service Access keys (SSA keys) which can be physically distributed in the form of a USB key with a Digi code (SSA hard keys) or remotely installed (SSA license key).
7. These TPMs are separate and apart from the protections or controls governing access to the Clinical Operation Software because they govern access levels to the Common Service Desktop only. Clinical Operations Software is accessible to any user once logged in. Common Service Desktop has a range of tools: Class A (referred to externally as General Service) for general service required by regional laws and regulations (e.g., AIAT regulations in the U.S. and regional laws) required to return the equipment to an operational state in accordance with GE HealthCare specifications (e.g., basic startup/installation instructions and AIAT guidelines or equivalent). Class A is available publicly, including to independent service organizations (Class A1 service software is accessible on the device without needing any additional keys or licenses; Class A2 and A3 service software is licensed on request with some regions charging a reasonable fee and others, like the U.S., providing the license at no additional charge). Class C (externally referred to as Technical Service) contains productivity and efficiency software and is only made available via sale and license to entitled customers and channel partners under contract with GE HealthCare. Finally, Common Service Desktop contains Class M software (externally referred to as GE HealthCare Highly Confidential) that is for GE HealthCare internal use only or has been identified as a GE HealthCare trade secret. Class M may be made available to channel partners under a channel partner agreement with GE HealthCare in some regions outside the U.S.
8. Access to the Clinical Operation Software is controlled by user credentials which are administered by the customer. By contrast, access to the System Servicing/Diagnostic Software Class C and M are controlled by the type of physical SSA USB key or digital license key installed in the system; by default, all Class A1 software will be accessible and other levels of software will be enabled based on installed key access level.
9. A person who has authorized access to the Clinical Operation Software does receive access to Class A1 System Servicing/Diagnostic Software by default; those tools are used for daily calibration activities such as tube calibration or warm up. For elevated access, the person or organization must license the key from GE HealthCare as described in Section 7 above.

10. These access controls serve purposes including, for example, safety of operation, system integrity, subscription-based offering, and protection of proprietary material.

IV. LICENSING, SERVICE OFFERINGS

11. GE HealthCare licenses access to its System Servicing/Diagnostic Software separately from the sale or lease of the device. Access to Class A2/A3 is made available to any customer or independent service organization through licensing. Access to Class C1/C2/C3 is made available to any customer through a service agreement or licensing.
12. The consideration charged for such access depends on the commercial policy of the country. The access provided may include licenses to Common Service Desktop restricted tools, training and/or support.
13. Customers may obtain maintenance or repair services through GE HealthCare, independent service organizations, their in-house service departments, and sometimes other manufacturers. If additional software access or expertise is required beyond the access already provided in Class A1, those parties can contact GE HealthCare to determine what licensing options are available.

V. MAINTENANCE-RELATED DOCUMENTATION

14. GE HealthCare publicly provides Maintenance-Related Documentation that includes detailed Class A1 service manuals containing step by step procedures, schematics and pictures on its online manual & documents website: <https://www.gehealthcare.com/en-us/support/manuals>
15. Clinical Operation Software and System Servicing/Diagnostic Software are documented in the product User/Operator manual and Service Manual, both available on the above website.
16. Maintenance-Related Documentation is used by operators, independent service organizations, GE HealthCare's channel partners and GE HealthCare when operating, installing or servicing the equipment.
17. Access to Class A1 documentation is public just like Clinical Operation documentation (also called operator manual).
18. GE HealthCare licenses access to Class A2/A3/C1/C2/C3 documentation, which GE HealthCare makes available and conditioned to an active licensing or service agreement.

VI. UNAUTHORIZED ACCESS AND PRACTICAL EFFECTS

19. GE HealthCare has encountered unauthorized access, distribution and use involving System Servicing/Diagnostic Software or Maintenance-Related Documentation. GE HealthCare

enforces against unauthorized use of its System Servicing/Diagnostic Software, SSA keys and Maintenance-Related Documentation through means such as cease-and-desist letters.

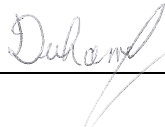
20. Unauthorized circumvention of the TPMs described above could grant unauthorized access to systems and compromise system integrity which could in turn compromise operator and patient safety and lead to wrong diagnosis.

VII. CONCLUSION

21. The Clinical Operation Software, System Servicing/Diagnostic Software, and Maintenance-Related Documentation described above are distinct in function and are subject to distinct access controls. Clinical Operation Software and Class A1 System Servicing/Diagnostic Software is controlled through user login. Access to Class A2/A3/C1/C2/C3 is dependent on the license key installed in the system. Access to Class M is limited to GE Healthcare internal as it is deemed highly confidential. As noted above, in some regions outside the U.S., Class M may be made available to channel partners under an agreement with GE HealthCare.
22. Class A2/A3/C1/C2/C3 System Servicing/Diagnostic Software and/or Maintenance-Related Documentation is made available through licenses or service agreements, and servicing of medical devices is performed by GE HealthCare, its channel partners, independent service organizations, in-house service departments of end-users, and other manufacturers.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on September 28th, 2026, in Buc, France

Signature: 

Print Name: Jerome Duhamel

Title: Global Service Operations GM

Company Name: GE Medical Systems SCS

EXHIBIT C

Declaration submitted in support of Comments from:

Advanced Medical Technology Association (AdvaMed)

1301 Pennsylvania Ave NW, Ste 400

Washington, DC 20004

DECLARATION OF PIERRE MALBOEUF

I, Pierre Malboeuf declare as follows based on my personal knowledge:

I. DECLARANT AND COMPANY BACKGROUND

1. I am the Vice President, Service Delivery of Hologic Inc. (“Hologic”). I have held this position since 2023. My responsibilities include service delivery of Hologic Technical and Field Service support to both customers and Hologic personnel. Product and software design are inherent to the products Hologic manufactures, distributes, and services.
2. I have 29 years of experience in Service Operations and Field Services. In my role, I am familiar with the company’s medical devices, clinical operation software, system servicing and diagnostic software, Maintenance-Related Documentation, access controls, licensing practices, and service offerings described below.
3. Hologic develops, manufactures, sells, and/or leases innovative medical technologies that effectively detect, diagnose and treat health conditions used for disease detection in breast health, gynecological health, sexual health, body composition, and skeletal health.

II. RELEVANT SOFTWARE AND MATERIALS

As used in this declaration:

- (a) “Clinical Operation Software” means software that health care professionals use to operate a medical device to perform patient care activities;
 - (b) “System Servicing/Diagnostic Software” includes software applications, diagnostic tools, calibration programs, configuration utilities, service interfaces, and related digital resources used to install, inspect, calibrate, test, maintain, diagnose, troubleshoot, update, or repair a medical device to its intended performance and safety specifications; and
 - (c) “Maintenance-Related Documentation” is non-software, digital work used for servicing, such as digital service manuals or repair procedure documentation.
4. Hologic uses Clinical Operation Software on Breast Health platforms to enable clinicians to diagnose and treat breast cancer.
 5. Hologic uses System Servicing/Diagnostic Software for those devices, including company-designed calibration and software service tools. This software is used to assist the service

technician in problem diagnosis, calibration assistance, and allows for the calibration of the mechanical and imaging sections of the product.

III. TECHNOLOGICAL PROTECTION MEASURES (TPMs) AND DIFFERENTIAL ACCESS

6. Access to the System Servicing/Diagnostic Software is controlled by passwords, license keys, license controls.
7. These TPMs are separate and apart from the protections or controls governing access to the Clinical Operation Software because they are separate software applications and have different access controls.
8. Access to the Clinical Operation Software is controlled by passwords and license controls controlled by clinical users. By contrast, access to the System Servicing/Diagnostic Software is controlled by passwords, license keys, license controls, and USB security devices.
9. A person who has authorized access to the Clinical Operation Software does not thereby receive authorized access to the System Servicing/Diagnostic Software. To obtain such access, the person or organization must contact Hologic Technical Support, where credentialing is verified for proper access allowance and safety control.
10. These access controls serve purposes including safety, system integrity, cybersecurity, protection of proprietary materials, and license management.

IV. LICENSING, SERVICE OFFERINGS, AND DISTINCT MARKET

11. Hologic can sell or provide access to its System Servicing/Diagnostic Software separately from the sale or lease of the device. Access is offered to factory-trained and authorized service personnel through service program offerings which provide credentialing.
12. The consideration charged for such access is determinable across type of customer, access needed, and other economic factors of install base support scale. The access provided may include calibration guided assistance as well as access to troubleshooting reference materials.
13. The market for these works and services includes hospital service personnel (BMETs) or third-party authorized service providers. Hologic competes in servicing and repairing these devices with other OEMs and ISOs, including GE Healthcare, Siemens Healthcare, Trimedx, Crothall, 626 Holdings, Cassling, Aramark, and Frontier.
14. Customers may obtain maintenance or repair services through OEM service or ISO service. If additional authorized software access or expertise is required, customers may request a limited use license via one-time charge or provide credentialing that entitles access via factory-provided technical instruction.

V. MAINTENANCE-RELATED DOCUMENTATION

15. Hologic provides Maintenance-Related Documentation that includes Service Manuals, User Manuals, Quality Control Manuals and required safety updates.
16. This documentation is stored in hard copy format with every shipped product. Relative to the Clinical Operation Software and System Servicing/Diagnostic Software, it is separated at the product level.
17. The documentation is used by authorized service providers when performing service and calibration requirements and for the purpose of restoring or maintaining the product to the manufacturer's specifications.
18. Access to this documentation is controlled by passwords and license controls. These measures are separate and apart from protections governing Clinical Operation Software because they are separate from the clinical software and are distinct from both clinical and service operations.
19. Hologic offers factory authorized training and credentialing access to this documentation through various entitlements based on customer need, demand, and partnership in post-warranty agreements.

VI. UNAUTHORIZED ACCESS AND PRACTICAL EFFECTS

20. Unauthorized circumvention of the TPMs described above could jeopardize system integrity, calibration of radiation releasing components, and provide for unsafe patient conditions.
21. Authorized access to System Servicing/Diagnostic Software and Maintenance-Related Documentation is available through factory-provided service manuals, and via factory-authorized training and license access subject to conditions of Hologic Learning and Development.

VII. CONCLUSION

24. The Clinical Operation Software, System Servicing/Diagnostic Software, and Maintenance-Related Documentation described above are distinct in function and are subject to different and distinct access controls.
25. System Servicing/Diagnostic Software and/or Maintenance-Related Documentation is monetized through Hologic Surecare Agreements and participants in this market that include direct customers, third-party service providers, and OEMs.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on 9.24.26 in Pittsburgh, PA

/s/ Pierre Malboeuf

Pierre Malboeuf
Vice President, Service Delivery
Hologic, Inc.

EXHIBIT D

Declaration submitted in support of Comments from:

Advanced Medical Technology Association (AdvaMed)

1301 Pennsylvania Ave NW, Ste 400

Washington, DC 20004

DECLARATION OF JACQUELINE DICKSON

I, Jacqueline Dickson, declare as follows based on my personal knowledge:

I. DECLARANT AND COMPANY BACKGROUND

1. I am the CSIP Services Operations Director of Philips North America LLC (“Philips”). I have held this position since 2024. My responsibilities include oversight and support relating to service governance, access management, investigations, compliance activities, and cross-functional escalation management. These responsibilities require regular interaction with personnel from service, cybersecurity, privacy, legal, regulatory, and business organizations, and provide me with direct knowledge of the policies, procedures, and operational controls relevant to the matters discussed in this declaration.

2. I have 22 years of experience in service operations related to medical devices, with a focus on governance and administration of service documentation and service applications. In my role, I am familiar with Philips’ medical devices, clinical operation software, system servicing and diagnostic software, Maintenance-Related Documentation, access controls, licensing practices, and service offerings described below.

3. Philips develops, manufactures, sells, and/or leases a comprehensive portfolio of medical systems including medical imaging systems (e.g., magnetic resonance imaging (MRI), computed tomography (CT), ultrasound systems, diagnostic x-ray (radiography and fluoroscopy), and image-guided therapy systems for angiography).

II. RELEVANT SOFTWARE AND MATERIALS

4. As used in this declaration:

- (a) “Clinical Operation Software” means software that health care professionals use to operate a medical device and to perform patient care activities;
- (b) “System Servicing/Diagnostic Software” includes software applications, diagnostic tools, calibration programs, configuration utilities, service interfaces, and related digital resources used to install, inspect, calibrate, test, maintain, diagnose, troubleshoot, update, or repair a medical device to its intended performance and safety specifications; and

(c) “Maintenance-Related Documentation” is non-software, digital work used for servicing, such as digital service manuals or repair procedure documentation.

5. Philips uses Clinical Operation Software on its medical imaging systems to enable clinicians to operate the device’s medical features and to access patient information in the course of patient care. Devices typically have two or more types of accounts for the Clinical Operation Software, including a login for technologists to access the clinical interface and patient information, and an information technology or hospital administration account used to configure clinical user accounts.

6. Philips uses System Servicing/Diagnostic Software for those devices. That software is proprietary to Philips and is used to perform various service tasks on the devices, including but not limited to system diagnostics, system installation, and system configuration. Some of that software may be used to check systems for errors, access system diagnostic information and service logs, perform system calibration or troubleshooting, verify device operation, modify device configurations (e.g., radiation dose), and customize devices. These service software tools are divided into categories that Philips calls “Levels.” Access to the tools in each Level is protected by TPMs and is governed by different terms and conditions, as described below.

III. TECHNOLOGICAL PROTECTION MEASURES (TPMs) & DIFFERENTIAL ACCESS

7. Philips uses several TPMs to control access to its System Servicing/Diagnostic Software. The principal measure is Philips’ proprietary Integrated Security Tool (“IST”), which controls both authentication and entitlement. Through IST, Philips applies encrypted certificates together with multifactor authentication to the device. The user must present a physical smartcard, which uses a proprietary program, in order to present the medical device with an encrypted, time-limited, user-specific certificate, and the user must enter the matching password for that specific user account. Upon successful login, the system presents only the service software tools that the user is entitled to use, based on the user’s IST entitlements.

8. These TPMs are separate and apart from the protections or controls governing access to the Clinical Operation Software. The Clinical Operation Software is managed separately. Its logins are username and password based, more like a Windows-type login, and they do not involve the IST smartcard, the encrypted user-specific certificate, or the entitlement system that determines which service software tools a user may access.

9. Access to the Clinical Operation Software is controlled by the technologist and information technology or hospital administration accounts described above, which are administered by the health care facility that owns or leases the device and its information technology personnel. Those logins are not in place to protect copyrighted material; they

are in place to allow device owners to ensure that only hospital-authorized clinical staff or other individuals can access a system's medical features and/or patient data. By contrast, access to the System Servicing/Diagnostic Software is controlled by the IST smartcard, the encrypted user-specific certificate, the matching account password, and the user's IST entitlements, each of which is issued and administered by Philips.

10. A person who has authorized access to the Clinical Operation Software does not thereby receive authorized access to the System Servicing/Diagnostic Software. A system owner is not authorized to access the protected System Servicing/Diagnostic Software, so it has no authority to authorize others to access or use such proprietary Philips software. To obtain such access, the person or organization must satisfy the conditions that apply to the Level of the tool sought. Level 0 tools are available to any person, including independent service organizations ("ISOs") or hospital biomedes, on request. Level 1 tools are available to hospital biomedes under a license granted as part of certain cooperative service agreements that include license fees, and subject to specific terms and conditions, including completion of Philips service training for that product and execution of a non-disclosure agreement. Level 2 tools are not available for licensing and are reserved for trained Philips engineers. Level 3 tools present an even greater risk if used with insufficient training and are likewise not available for licensing and are restricted to a small number of more highly trained and experienced service specialists.

11. These access controls serve purposes including protecting proprietary Philips software, patient and servicer safety, the performance and cybersecurity of the device, and license management. All Levels contain proprietary software developed by Philips and should only be used by sufficiently trained individuals given the safety-critical nature of medical device servicing. Level 2 and Level 3 in particular contain tools that are highly proprietary, pose a greater risk to patient or servicer safety, or that can alter or impact the performance or cybersecurity of the device. The strict restrictions Philips places on these tools are in line with FDA guidelines for remanufacturing and cybersecurity for medical devices.

IV. LICENSING, SERVICE OFFERINGS, AND DISTINCT MARKET

12. Philips licenses access to its System Servicing/Diagnostic Software separately from the sale or lease of the device, on terms that correspond to the Level of the tool. Philips provides Level 0 access to ISOs, hospital biomedes, and others on request. Philips licenses Level 1 access to hospital biomedes under certain cooperative service agreements, subject to requirements for system-specific service training and non-disclosure agreements. Level 2 and Level 3 access is not available for license and is retained for Philips.

13. Access is offered both through separate service agreements and through licensing. The consideration charged for Level 1 access takes the form of license fees included in

certain cooperative service agreements. The access provided includes the licensed service software tools themselves, the IST credentials and encrypted certificate required to authenticate to them, the IST entitlements that determine which tools the licensee may use, and access to the Maintenance-Related Documentation described below at the corresponding Level.

14. The market for these works and services includes hospital biomedical engineering departments that license the Level 1 works as part of certain cooperative service agreements, and Philips' own engineers and service specialists, for whom the Level 2 and Level 3 works are reserved and whose tools support Philips' own service activities. Philips competes in servicing and repairing these devices with ISOs, other OEMs, and in-house biomedes. In the FDA's 2018 report, "FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices," the FDA estimated that over 16,000 firms perform medical device service in the United States.

15. Customers may obtain maintenance or repair services from whomever they chose, including Philips, their own in-house biomedical engineering personnel, ISOs, or other OEMs. If additional authorized System Servicing/Diagnostic Software access or expertise would assist with a service, the customer or servicer may request Level 0 tools, or, in the case of hospital biomedes, may obtain a license to Level 1 tools as part of a cooperative service agreement upon completion of Philips service training for that product and execution of a non-disclosure agreement. Use of Level 2 or Level 3 tools is for servicing is reserved for Philips.

V. MAINTENANCE-RELATED DOCUMENTATION

16. Philips provides Maintenance-Related Documentation, which is likewise organized by Level. Basic maintenance manuals are available at Level 0 on request. More advanced documentation is available at Level 1 under license, subject to training and confidentiality requirements. Level 2 documentation poses additional safety, cybersecurity, or remanufacturing risks and is limited to Philips only.

17. This documentation is nearly exclusively stored on a cloud server and is not stored on the medical device. It is therefore maintained separately from both the Clinical Operation Software and the System Servicing/Diagnostic Software that reside on the device, and it is accessed through a Philips-hosted cloud server (InCenter) rather than through the device's clinical interface.

18. The documentation may be used by those performing service, including ISOs, hospital biomedes, and Philips personnel, with access on demand, based on a user's entitlements, at the time of need.

19. Access to this documentation is controlled by TPMs. Philips uses the proprietary IST to protect the login for service documentation, and multifactor authentication is required: the user must log in to the IST application on their computer to activate the encrypted certificate, and must use the IST account to log in to the cloud server (InCenter). The certificate is valid only on that user's computer; a user cannot log in from a different computer without re-registering with IST. Once logged in, the server presents only the materials that match the user's entitlements. To open protected Level 1 or higher materials, which are encrypted, the IST application must be active and logged in on the computer, and the tool then decrypts the documentation for viewing. These protection measures prevent the protected documents from being downloaded, saved, or printed. Level 0 documentation requires a login using IST credentials but is not encrypted, and select documents, such as Instructions for Use for the medical devices, are available with a "guest" login and are not subject to these additional protections. These measures are wholly separate and apart from the logins used for the Clinical Operation Software, because IST credentials, certificates, and entitlements are issued and controlled by Philips, whereas the Clinical Operation Software logins are username and password accounts administered by the health care facility and its information technology personnel.

20. Philips offers access to this documentation separately from the sale or lease of the device, on terms that correspond to the Level of the material: Level 0 maintenance manuals are available to any person, including ISOs and hospital biomedics, on request; more advanced Level 1 documentation is available under license, subject to completion of Philips service training for the product and execution of a non-disclosure agreement; and Level 2 documentation is not offered for license and is limited to Philips.

VI. UNAUTHORIZED ACCESS AND PRACTICAL EFFECTS

21. Philips enforces against unauthorized use of, and infringement relating to, its System Servicing/Diagnostic Software, service keys, and Maintenance-Related Documentation. Philips enforces both through more informal means, such as cease-and-desist letters, and through more formal means, up to and including litigation. Philips has obtained judgments in multiple litigations, including against Transtate/Avante, KPI Ultrasound, and Image Technology.

22. Unauthorized circumvention of the TPMs described above would permit persons who have not completed Philips service training for the product, and who are not subject to the license terms and non-disclosure agreements under which Philips grants access, to obtain access to the System Servicing/Diagnostic Software and the Maintenance-Related Documentation. That includes the Level 2 and Level 3 tools and the Level 2 documentation that Philips does not license to anyone, which are highly proprietary, pose

a greater risk to patient or servicer safety, or can alter or impact the performance or cybersecurity of the device.

23. Based on my responsibilities and experience, authorized access to Philips' service software and Maintenance-Related Documentation is available through IST and, in the case of documentation, through the InCenter cloud server, subject to the conditions that apply to each Level: Level 0 tools and documentation are provided on request, and Level 1 tools and documentation are licensed to hospital biomedics as part of certain cooperative service agreements that include license fees, completion of Philips service training for that product, and execution of a non-disclosure agreement.

VII. CONCLUSION

24. The Clinical Operation Software, System Servicing/Diagnostic Software, and Maintenance-Related Documentation described above are distinct in function and are subject to distinct access controls. The Clinical Operation Software is protected by username and password accounts administered by the health care facility and its information technology personnel, and those accounts exist to control who may access the device's medical features and patient data. The System Servicing/Diagnostic Software and Maintenance-Related Documentation are protected by Philips' proprietary Integrated Security Tool, which requires a physical smartcard, an encrypted user-specific certificate, and the matching account password, and which presents only those tools and materials that match the user's Philips-issued entitlements.

25. The System Servicing/Diagnostic Software and Maintenance-Related Documentation are monetized through the license fees charged for Level 1 access as part of certain cooperative service agreements with hospital biomedical engineering departments, subject to service training and non-disclosure requirements, and they participate in a market that includes ISOs, other OEMs, and in-house biomedics — a market in which the FDA estimated in 2018 that over 16,000 firms perform medical device service in the United States.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on September 28, 2026 in Highland Heights, Ohio.

/s/ Jacqueline M. Dickson

Jacqueline Dickson
CSIP Services Operations Director
Philips North America LLC

EXHIBIT E

Declaration submitted in support of Comments from:

Advanced Medical Technology Association (AdvaMed)

1301 Pennsylvania Ave NW, Ste 400

Washington, DC 20004

DECLARATION OF GONCALO ARNAUT

I, Goncalo Arnaut, declare as follows based on my personal knowledge:

I. DECLARANT AND COMPANY BACKGROUND

1. I am the Head of Customer Services for North America at Siemens Medical Solutions USA, Inc. (“Siemens Healthineers”). I have held this position since 2024. My responsibilities include oversight of customer service operations for Siemens Healthineers medical imaging systems in North America, including service delivery, maintenance and repair support, service-related software access, service key administration, technical training and credentialing requirements, cybersecurity considerations related to service activities, and the protection and appropriate use of proprietary service materials.

2. I have been with Siemens Healthineers for 22 years, having worked in the field of customer services for medical imaging equipment since 2013. In my role, I am familiar with Siemens Healthineers’ medical devices, Clinical Operation Software, System Servicing/ Diagnostic Software, Maintenance-Related Documentation, access controls, licensing practices, and service offerings as described below.

3. Siemens Healthineers develops, manufactures, sells, and/or leases medical imaging devices and systems, including for x-ray imaging, molecular imaging, computed tomography (CT) imaging, magnetic resonance (MR) imaging, and angiography imaging used for diagnosis in clinical applications including for detection of abnormalities, to track disease, and/or visualize the anatomy of the patient in clinical fields including oncology, cardiology, neurology, and women’s health.

II. RELEVANT SOFTWARE AND MATERIALS

4. As used in this declaration:

- (a) “Clinical Operation Software” means software that health care professionals use to operate a medical device to perform patient care activities;
- (b) “System Servicing/Diagnostic Software” includes software applications, diagnostic tools, calibration programs, configuration utilities, service interfaces, and related digital resources used to install, inspect, calibrate, test, maintain,

diagnose, troubleshoot, update, or repair a medical device to its intended performance and safety specifications; and

- (c) Maintenance-Related Documentation is non-software, digital work used for servicing, such as digital service manuals or repair procedure documentation.

5. Siemens Healthineers uses Clinical Operation Software on its imaging devices to enable clinicians to operate the device for patient use. Access to the Clinical Operation Software is typically through an operator login account followed by a password, and accounts can be created on the device for each user.

6. Siemens Healthineers uses System Servicing/Diagnostic Software on its imaging devices. This software provides information, data, and tools that pertain to the performance of the device itself. It can provide an individual with access to certain diagnostic tests that can be performed on the system, it can monitor hardware and component status, and it can output error codes and logs. It can also support assembly, installation, adjustment, and calibration, in addition to testing and diagnosing a system for maintenance and repair. For some Siemens Healthineers imaging devices, most of the System Servicing/Diagnostic Software is hosted on the cloud, separated physically from the imaging device and from the Clinical Operation Software on the imaging device.

III. TECHNOLOGICAL PROTECTION MEASURES (TPMs) & DIFFERENTIAL ACCESS

7. Access to Siemens Healthineers' System Servicing/Diagnostic Software generally requires a service key. The key is a character string, generally 256 characters, that is entered at the user interface of the System Servicing/Diagnostic Software. The character string for the key may be updated and is checked for approval for usage on the System Servicing/Diagnostic Software, and a key may be approved for access for a set period, such as days or weeks. Service keys are provided at various levels to access certain information or tools within the System Servicing/Diagnostic Software, and generally can be categorized at basic, advanced, and proprietary levels. A service key is typically generated using information pertaining to the imaging device, as for example from the imaging device workstation, and can also be generated based on information provided via a dongle, which is a physical device often connected over USB.

8. These TPMs are separate and apart from the protections or controls governing access to the Clinical Operation Software. The TPM for the Clinical Operation Software, which is used to operate the device for patient use, is typically an operator login account followed by a password, and accounts can be created on the device for each user. The service key is a distinct measure: following login to the device through the Clinical Operation Software, the user must navigate to a service menu item and then access to the System Servicing/Diagnostic Software at its own user interface requires input of the

service key. For some imaging devices, most of the System Servicing/Diagnostic Software is also hosted on the cloud, physically separated from the imaging device and from the Clinical Operation Software that resides on it.

9. Access to the Clinical Operation Software is controlled by the operator login account and password. That login and password are initially provided to the customer by Siemens Healthineers, and the customer operating the system for patient use then controls login and password access. By contrast, service keys are distributed and approved by Siemens Healthineers. The distribution and availability of service keys for a system depends on the category of the service key and, for advanced service keys, on eligibility criteria such as training and contract terms.

10. Access to the Clinical Operation Software does not thereby provide for automatic access to the System Servicing/Diagnostic Software. An operator login permits a user to reach the service menu item, but access to the System Servicing/Diagnostic Software itself requires a service key distributed and approved by Siemens Healthineers at the level corresponding to the information or tools sought. For advanced service keys, the person or organization must also satisfy eligibility criteria such as training and contract terms.

11. These access controls serve several important purposes. They support patient safety and device integrity by helping ensure that the Clinical Operation Software is accessible only to customer-designated users and that certain service functions are performed by appropriately trained and qualified personnel. They also reduce cybersecurity risks associated with unauthorized access to the Clinical Operation Software and the System Servicing/Diagnostic Software. In addition, the controls protect proprietary service information and tools, support the administration of software licenses and contractual access rights, and reduce the risk that unauthorized or inappropriate service activities of which could affect the safe and proper clinical operation of the imaging system.

IV. LICENSING, SERVICE OFFERINGS, AND DISTINCT MARKET

12. Siemens Healthineers licenses usage of its System Servicing/Diagnostic Software at certain levels separately from the sale of the device. Access can be made available to the device owner upon system purchase or at a later time and can also be licensed at certain levels to other servicing organizations. Service keys to access the System Servicing/Diagnostic Software are provided depending on the level required and the license contract.

13. Access is offered both through separate service agreements and through licensing wherein then the service keys can be made available. The term of a license for service key use can be short, for example a few days, or long term, as for example annually. Service keys can be provided at no charge for certain levels, depending on the tasks required.

14. The market for these works and services is a post-sale market that arises after the sale of the imaging system itself and is intended to keep the equipment maintained and working. Participants in that market include customers that purchased an imaging system and that may also obtain or purchase service keys for access to service the system, as well as independent service organizations and manufacturer service technicians that seek to acquire or obtain such access. Siemens Healthineers competes in servicing and repairing these devices with independent service organizations, self-service parties such as hospital in-house service departments, and other manufacturers that also provide service.

15. Customers may obtain maintenance or repair services from Siemens Healthineers, from their own in-house service personnel, from independent service organizations, or from other manufacturers that provide service. If additional authorized System Servicing/Diagnostic Software access or expertise is required, the customer or servicer may obtain a service key at the applicable level through a license agreement or service contract with Siemens Healthineers, subject, for advanced service keys, to meeting eligibility criteria such as training and contract terms.

V. MAINTENANCE-RELATED DOCUMENTATION

16. Siemens Healthineers provides Maintenance-Related Documentation, which includes service manuals and other technical documentation used to service a system.

17. This documentation is typically separate from the Clinical Operation Software and the System Servicing/Diagnostic Software. It is usually stored in an electronic library on a website, with certain access controls for non-public information. Some older imaging systems store Maintenance-Related Documentation directly on the system.

18. The documentation is used to repair Siemens Healthineers imaging systems. Access to the Maintenance-Related Documentation for service and repair is granted by Siemens Healthineers and allows an account to be created on the website. Access may be provided to customers, to service organizations, or to Siemens Healthineers technicians. Some Maintenance-Related Documentation is provided publicly from the website without access controls.

19. Access to the non-public Maintenance-Related Documentation on the website is controlled by login and password, which are provided by permission from Siemens Healthineers. For non-public Maintenance-Related Documentation stored on older imaging systems, a service key provides access. These measures are separate and apart from the protections governing the Clinical Operation Software: the website login and password are different from the Clinical Operation Software login and password on the imaging device itself, and website access is granted by Siemens Healthineers, whereas the Clinical Operation Software login and password are controlled by the customer after Siemens Healthineers initially provides them.

20. Siemens Healthineers provides access to this documentation separately from the sale of the device, by granting an account on the website to customers, service organizations, and Siemens Healthineers technicians.

VI. UNAUTHORIZED ACCESS [AND PRACTICAL EFFECTS]

21. Unauthorized circumvention of the TPMs described above would permit persons who have not obtained a service key distributed and approved by Siemens Healthineers, and who have not satisfied the eligibility criteria such as training and contract terms that apply to advanced service keys, to access the System Servicing/Diagnostic Software and the non-public Maintenance-Related Documentation.

VII. CONCLUSION

22. The Clinical Operation Software, System Servicing/Diagnostic Software, and Maintenance-Related Documentation described above are distinct in function and are subject to distinct access controls. The Clinical Operation Software is protected by an operator login account and password that Siemens Healthineers initially provides to the customer and that the customer thereafter controls. The System Servicing/Diagnostic Software is protected by a service key — a character string, generally of 256 characters, generated from information pertaining to the imaging device or provided via a dongle, approved for a defined period, and issued at basic, advanced, or proprietary levels — which Siemens Healthineers distributes and approves. The non-public Maintenance-Related Documentation is protected at a website through login and password which is granted by Siemens Healthineers and, on older imaging systems, by a service key.

23. Usage of the System Servicing/Diagnostic Software is monetized through licenses providing service key access at certain levels, made available through license and service contracts with terms ranging from a few days to a year, and it participates in a post-sale market for keeping imaging equipment maintained and working — a market that includes device owners, independent service organizations, hospital in-house self-service parties, other manufacturers that provide service, and Siemens Healthineers' own service technicians.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on September 25, 2026, in Cary, North Carolina.



Electronically signed by: GONCALO
Arnaut
Reason: I am the author of this
document
Date: Sep 25, 2026 13:16:55 EDT

Goncalo Arnaut
Head of Customer Services for North America - Siemens Healthineers