MITA
MEDICAL IMAGING
& TECHNOLOGY ALLIANCE
A DIVISION OF NEMA

1300 North 17th Street ▪ Suite 900
Arlington, Virginia 22209
Tel: 703.841.3200
Fax: 703.841.3392
www.medicalimaging.org

December 1, 2022

The Honorable Mark Warner
703 Hart Senate Office Building
Washington, DC 20510

Re: Cybersecurity is Patient Safety – Policy Options in the Health Care Sector

Dear Senator Warner,

The Medical Imaging & Technology Alliance (MITA) is the leading trade association representing the manufacturers of medical imaging equipment and radiopharmaceuticals, and we appreciate your work to promote healthcare sector cybersecurity in pursuit of patient safety. MITA has for many years championed the need for health care sector stakeholders to embrace the concept of "Shared Responsibility" to achieve stronger cybersecurity. We applaud "Cybersecurity is Patient Safety: Policy Options in the Health Care Sector" as a strong step towards such a goal. The following comments reflect our mutual commitment towards this outcome, and we look forward to continuing to work with you and your staff to contribute alongside other stakeholders on any policy options as they evolve.

1.1 HEALTH CARE CYBERSECURITY LEADERSHIP WITHIN THE FEDERAL GOVERNMENT

The Healthcare Sector Coordinating Council Cybersecurity Working Group (HSCC Cyber WG), in coordination with the Department of Health and Human Services (HHS), has produced a wide range of actionable resources for healthcare stakeholders since its inception in 2018. The cross-sector public-private partnership has produced important documents such as the "Medical Device and Health IT Joint Security Plan" (JSP), the "Health Industry Cybersecurity Practices" (HICP) guide series, and the "Model Contract-Language for Medtech Cybersecurity" (MC2). A full list of publications is available at the HSCC Cyber WG website[1].

HHS' support of the HSCC Cyber WG is very important to continued progress in healthcare sector cybersecurity. The HSCC Cyber WG brings industry representatives, healthcare providers, and federal regulators together in an appropriate forum to discuss a wide range of cyber-related problems and to generate consensus-based solutions. This will become even

[1] https://healthsectorcouncil.org/hscc-publications/

more important as cybersecurity concerns continue to grow. We encourage continued support of HHS and the HSCC Cyber WG as the appropriate, designated cybersecurity leadership entity for health care within the federal government.

1.2 PROTECTING HEALTH CARE RESEARCH AND DEVELOPMENT FROM CYBERATTACKS

Cybersecurity threats to healthcare research go beyond those traditionally attributed to activities such as corporate espionage and nation-state activity. Exploited vulnerabilities and active cyber-attacks for any purpose can expose sensitive intellectual property (IP) and weaken the target device against future attacks. It is critical for policy and guidance which looks to protect healthcare IP address this issue by taking a consistent stance against attacks of any kind, including those which would "bypass" security components and mitigations incorporated into devices to access sensitive files or proprietary tools.

1.3 HEALTH CARE SPECIFIC GUIDANCE FROM THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

MITA members use the NIST Cybersecurity Framework (CSF) among other resources when they develop cybersecurity programs for their organizations. The CSF provides a comprehensive roadmap for adapting and adopting cybersecurity procedures and tools to a wide range of industries. The CSF excels in its ability to normalize conversations about cybersecurity maturity and expectations between industries, and between stakeholders within industries.

However, the HSCC Cyber WG is the appropriate organization to produce health care specific guidance for cybersecurity. The sole focus for the HSCC Cyber WG is health care cybersecurity, and the large community of dedicated members enables a much more specified and comprehensive approach to cybersecurity in the space. In fact, the HSCC Cyber WG has already generated several well-received and well-utilized health care specific cybersecurity frameworks, such as the Joint Security Plan.

1.4 MODERNIZING HIPAA TO ADDRESS CYBER THREATS

HIPAA is focused on portability and privacy. Its legacy in health care regulations is long, and the law is effective in addressing those issues which it was designed to address. We agree that the law does not necessarily cover the full spectrum of cybersecurity concerns we face in our modern environment. However, we do not believe that revising HIPAA is the best way to address this problem.

Any significant changes to HIPAA would necessarily be a long, complicated process that would have a substantial administrative impact on all stakeholders in the healthcare sector. Rather than overhaul HIPAA and force stakeholders to change their current practices for portability and privacy, we recommend that cybersecurity guidelines and policy be

considered separately. This is especially true as other technologies (such as Artificial Intelligence) force industries and policy makers to grapple with the interplay between cybersecurity, confidentiality, privacy, and bias. Separating cybersecurity will enable improvements without risking unintended consequences or confusion.
It's also imperative that cyber policies and guidelines leverage consensus standards and guidance (like those created by the HSCC Cyber WG, ANSI, MITA, IMDRF, AAMI, ISO and IEC).

1.6 WORKFORCE DEVELOPMENT PROGRAM THAT FOCUSES ON HEALTH CARE CYBERSECURITY

Pursuit of workforce development programs should be a top priority. A multi-disciplinary effort that includes manufacturers, providers, and subject matter experts (SMEs) will be needed to encourage collective action and ensure that each stakeholder has the tools they need to perform their part.

Previous workforce development efforts have focused on the health care provider. But manufacturers, and other stakeholders, should not be overlooked. Shared responsibility necessitates that all actors in the health care space be informed about the expectations they have to fulfill, the processes and procedures to employ, and the tools to use. MITA members also recommend engaging manufacturer SMEs during the creation of curriculum and standards and expectations of any healthcare cybersecurity workforce development program. This will help to ensure that the training is up-to-date and teaches the skill sets needed to implement and support a comprehensive cybersecurity program for health care organizations. This is particularly important for certificate and continuing educational training programs to enhance a person’s existing cybersecurity credentials.

2.1 ESTABLISHING MINIMUM CYBER HYGIENE PRACTICES FOR HEALTH CARE ORGANIZATIONS

The HSCC Cyber WG has already created cyber hygiene documents for health care organizations and those documents should provide the basis for any oversight or compliance practices. The interconnected nature of health care organizations, device manufacturers, and other stakeholders such as payers suggests that HHS should remain the primary federal agency dedicated to any health care related practices. However, if oversight policies are pursued, responsibility for that oversight should not fall to the FDA. FDA responsibility should remain scoped to manufacturers. Expanding FDA oversight responsibility to health care organizations would strain agency resources and have severe impact on the review and approval process for innovative and life-saving technologies.

2.2 ADDRESSING INSECURE LEGACY SYSTEMS

There are two separate pursuits in addressing insecure legacy systems. One is to resolve the existing problems related to the use of devices past their manufacturer declared end of life date by health care organizations. The other is prevention of premature obsolescence due to circumstances beyond manufacturer control.

Take the premature obsolescence problem first. Medical equipment manufacturers are often dependent on large software companies (such as Microsoft) that provide the Operating Systems (OS) that many imaging medical devices are based on. The inadequately short duration for support of the OS version directly contributes to gaps between the physical equipment and software lifecycles. Equipment manufacturers are often forced to pass on the cost of misaligned life cycles to providers by way of upgrades. Congress should consider how to incentivize the software companies like Microsoft and the tech industry in general to better support critical infrastructure use cases (such as health care) rather than put new requirements on health care companies and manufacturers who have limited to no ability to influence large software company product lifecycles or tech company decisions directly.

For future devices, modular design can be effective in some cases. However, as with any design choice, the benefits modular design provides does not always outweigh the costs and cannot be relied on as the singular design improvement for all device types. Implementing designs using a modular architecture is simply infeasible for many medical device types. Modular design is more time intensive for developers, introduces points of failure at each modular connection point, can reduce configuration capabilities, could complicate interoperability between devices and supporting infrastructure, and often requires increased compute resource usage. These drawbacks mean modularity can be a non-starter for certain device types. Any policy which pushed modularity as the single-best design option would stifle innovation and necessarily put certain devices, manufacturers, and patients at a disadvantage.

The current install base provides a separate and distinct set of problems. New designs cannot be adapted to equipment which is already manufactured. In addition, hardware and design constraints can make it impossible to update older devices with new software. Replacement with new equipment (especially equipment over 10 years old) will provide the best solution to the cybersecurity problems presented by legacy devices.

It should be recognized that many legacy devices in the current install base can be run safely and securely even if they include software or hardware with identified vulnerabilities. Mitigations and external tools validated by the medical device manufacturer and appropriately implemented by the health care organization can enable potentially at-risk devices to perform their intended use. However, these mitigations and tools can quickly become complex to implement and maintain. This increases the operational cost to the health care organization, which can be reduced by replacing the old equipment with new equipment to take advantage of modern capabilities and tools.

The requirements for a “cash for clunkers” reimbursement policy have been a subject of much debate among manufacturers, health care organizations, and other stakeholders. The difficulty lies in the complex interplay between device design choices, mitigation decisions, available tools, and user capabilities. To select specific cybersecurity components (such as encryption capabilities, or firewall presence) as criteria for a reimbursement program runs a high risk of producing both false positives (where devices that do not need replacement qualify) and false negatives (where devices that do need replacement do not qualify).

Rather than identify specific criteria, MITA recommends that policy makers consider the age of the device as a proxy. Since the FDA published its first pre-market guidance on Cybersecurity in 2014, medical device manufacturers have had to meet new and escalating requirements related to the cybersecurity of their devices. This distinction—before the guidance publication and after—provides one reasonable demarcation for legacy replacement.

Policy makers should also understand that medical device manufacturers have limited control over third-party software update availability. Third-party software developers do not often consider interoperability with medical devices during development. This includes decisions made by third-party software developers about software-hardware compatibility, which can make software updates impossible without expensive hardware upgrades. Any requirements placed directly on manufacturers to provide software updates for any length of time will put those manufacturers at a disadvantage and, ultimately, raise costs for both manufacturers and health care organizations.

For instance, assume a medical device manufacturer is required to provide updates to software for 10 years. If the manufacturer cannot guarantee that a certain software will still be providing updates in 10 years, they will necessarily need to avoid that software. This creates a disincentive to use innovative and cutting-edge technologies in favor of older technologies—even if those technologies are no longer state of the art. Rather than focus on medical device manufacturer requirements, MITA again urges policy makers to address the underlying conflict between software company lifecycles and medical device lifecycles.

MITA urges policy makers to avoid right to repair policies which would ultimately reduce the cybersecurity posture for medical devices by increasing vulnerabilities and reducing controls. "Right to repair" is a complex topic that stretches far beyond questions of cybersecurity, health care IT, and legacy medical devices.

Cybersecurity concerns are predominantly a software issue that can only be addressed by SMEs with deep understanding and knowledge of proprietary software code that only the original equipment manufacturer possesses. MITA is deeply concerned that application of "right to repair" policies to FDA regulated medical devices would have significant unintended consequences, presenting new and unnecessary risks to patient and operator safety, device performance, cybersecurity, and market dynamics.

Knowledge of and compliance with FDA regulatory requirements is essential to performance of medical device servicing activities in a way that results in the safe and effective operation of the medical device. Operating within a quality management system as codified by FDA in 21 CFR 820: Quality System Regulation ensures that medical devices consistently meet applicable specifications and requirements. Currently, non-OEM medical device servicing operations are not required to implement quality management systems which conform with 21 CFR 820. ISOs have made expansive demands for proprietary servicing materials such as service manuals, software keys, schematics, and tools. These same businesses have consistently refused to implement even basic quality or safety controls. This raises

cybersecurity risk concerns related to the integrity and confidentiality of information, credentials, and other cyber-related resources.

Despite claims made by these businesses, adequate performance of medical device servicing activities is not dependent only on possession of certain materials. We want to ensure our devices to perform safely and effectively for patient care. Application of "right to repair policies" to FDA regulated medical devices would, unfortunately, work counter to this objective.

Whenever software is installed or adjusted for a medical device, or if software tools are used to access a device for diagnostic and maintenance purposes, the integrity of the software may be compromised. Unvalidated software without confirmed authenticity or system integration may present significant potential security vulnerabilities and operational issues. Additionally, expanded and uncontrolled access to medical device operating systems and software applications creates the potential for increased cybersecurity risks, as the opportunity to intentionally or unintentionally introduce security vulnerabilities to the device and to any networks to which the device is connected (e.g., hospital) also expands. More information about the conflicts between cybersecurity and right-to-repair can be found in our response to "Discussion Paper: Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities" produced by the FDA[2].

2.3 SOFTWARE BILL OF MATERIALS

Software Bill of Materials (SBOM) content must be as harmonized as possible across every sector to ensure value and viability. This necessitates that fewer requirement variations should be pursued. The health care environment deploys software and devices beyond those classified as medical devices, for example traditional IT or HVAC systems, all of which bring additional cyber risk and can benefit from the transparency made possible by SBOMs, so different approaches for different types of devices would ultimately harm health care organizations. Core SBOM requirements should be developed by a single body, such as NIST, and those requirements should provide a true minimum to which all sectors can adhere.

If deviations are needed, then those deviations should be discussed and determined within consensus bodies within the relevant sector. For health care, organizations like the HSCC Cyber WG, MITA, and AAMI could all be appropriate sources of consensus. Government policy and legislation should not be used to drive requirements for sub-sectors. Such a rigid approach would result in splintered adherence to SBOM requirements and reduce the usability and value of the SBOM.

Rather than consider questions of gravity in Health IT, MITA suggests that policy makers consider questions of access and availability. Healthcare SBOMs will necessarily be tied to adoption by other products (especially operating software) because of dependencies. SBOM requirements should not be applied retroactively because the administrative costs would be substantial, and because the information provided could not be confirmed as accurate or

[2] https://www.regulations.gov/comment/FDA-2021-N-0561-0015

useful. This would be of limited benefit when weighed against the substantial cost as compared to the value that would be achieved producing SBOMs for new equipment—especially when coupled with an equipment replacement policy.

For medical device manufacturers, SBOM creation (during device development) should be mandatory. The FDA should be able to confirm the existence of an SBOM document during submission, or during an inspection, but otherwise publication and sharing should be voluntary. SBOM contains detailed information about device design and, without careful controls, access to the SBOM can endanger IP and decrease competition. Outdated SBOMs archived in uncontrolled databases heightens risks for disinformation which leads to errors in cybersecurity decision-making.

There is a debate about the risks associated with wide-spread SBOM availability within the cybersecurity community. Some experts suggest that the "bad actors" are then able to obtain the information included in an SBOM easily and so providing it to the "good actors" is a net win. Other experts point to the reduced entry barriers for bad actors if information once protected by network and encryption controls is made absolutely transparent, increasing total threat vectors. MITA members believe that transparency can have a positive impact on cybersecurity and that sharing information can support each stakeholder in their security roles. However, it is critical that shared information be treated appropriately, and risks associated with that information be reduced—just like sensitive information in any risk-based process.

How an SBOM is shared, such as through a central repository, also has implications for value and risk. A repository managed by the government is not going to benefit health care organizations because they will want to have customized repositories that fit their environment. Centralized repositories also tend to lose relevance quickly as the information becomes out of date. Rather, MITA recommends that SBOM sharing and publication be determined through stakeholder consensus and individual business needs.

Finally, it should be recognized that SBOMs by themselves do not increase cybersecurity protection. It takes an organization with enough technological maturity and detailed software architecture knowledge to be able to interpret the information in the SBOM. Today, this is not always possible for many health care organizations. Even when the providers have the capability to analyze the SBOM, they don't have the detailed device design knowledge the manufacturer has, to be able to assess the level of risk, if any, that may be present. This context cannot be provided within the SBOM itself, but instead depends on other means of communicating risk, such as Vulnerability Exploitability eXchange (VEX).

2.5 FINANCIAL IMPLICATIONS FOR INCREASED CYBERSECURITY REQUIREMENTS

Ensuring cybersecurity in medical devices is a shared responsibility that requires investment from multiple parties. Policies should be implemented that ensure healthcare facilities are sufficiently well resourced to upgrade less cybersecure legacy medical devices and maintain the cybersecurity of existing installed base. Any payment policies tied to cybersecurity requirements need to be funded in addition to the existing Medicare fee schedules and their

payment methodologies. Otherwise, there is risk of unintended consequences for patients due to the budget neutrality constraints in the construction and annual rate-setting practices within the existing Medicare fee schedules.

3.1 CYBER EMERGENCY PREPAREDNESS

FDA already requires medical imaging devices to have a failsafe mode in the event of a connectivity failure. This mode enables the equipment to function offline for a period of time before the connection is restored.

These failsafe mechanisms are designed primarily to mitigate threats to the device itself. Other mechanisms, such as those which can be deployed in a health care organization network, could be considered in policies to improve resiliency.

3.3 DISASTER RELIEF PROGRAM

The definition of a "cyber disaster" must be strictly scoped. If cyber disaster is not legally differentiated from "cyber incident", or "cyber-attack", there would be substantial implications on manufacturers, health care organizations, insurers, and other stakeholders.

+++

MITA commends Senator Warner for his continued work on policies regarding health care sector cybersecurity. MITA and its members stand ready to assist in these efforts and look forward to our continued work together on any policy initiatives that develop. If you have any further questions or need additional information, please do not hesitate to contact Zack Hornberger, Director of Cybersecurity & Informatics at zhornberger@medicalimaging.org or by phone at 703-841-3285.

Sincerely,

Patrick Hope
Executive Director, MITA

MITA is the collective voice of medical imaging equipment and radiopharmaceutical manufacturers, innovators and product developers. It represents companies whose sales comprise more than 90 percent of the global market for medical imaging technology. These technologies include: magnetic resonance imaging (MRI), medical X-Ray equipment, computed tomography (CT) scanners, ultrasound, nuclear imaging, radiopharmaceuticals, radiation

therapy equipment, and imaging information systems. Advancements in medical imaging are transforming health care through earlier disease detection, less invasive procedures and more effective treatments. The industry is extremely important to American healthcare and noted for its continual drive for innovation, fast-as-possible product introduction cycles, complex technologies, and multifaceted supply chains. Individually and collectively, these attributes result in unique concerns as the industry strives toward the goal of providing patients with the safest, most advanced medical imaging currently available.