December 8, 2022

The Honorable Senator Mark R. Warner
US Senate
Washington DC
Via email: cyber@warner.senate.gov

Ref: Cybersecurity is Patient Safety policy paper

Dear Senator Warner:

This is to submit comments to the policy paper referenced above.

I. Introduction of Alliance

Before providing information and comments, please allow us to introduce the Alliance for Quality Medical Device Servicing (the "Alliance"). The Alliance is an informal coalition of the leading independent medical device service organizations which support healthcare delivery organizations ("HDOs") across the United States, namely TRIMEDX, Sodexo, Crothall, Agiliti, and the InterMed Group.

Alliance members collectively employ tens of thousands of associates across all fifty states and actively service and maintain millions of medical devices. The Alliance members, as independent service organizations ("ISOs"), offer to their HDO clients not only safe and effective service, but also an equipment agnostic perspective focused on ensuring safety, reliability, and efficiency.

The Alliance's mission is to advance policy solutions that will result in ensuring the safety and availability of medical devices for hospitals and lowering health care costs nationwide. The Alliance is working to continue to make ISOs a cost-effective solution for providers, which ultimately improves the safety and quality of patient care.

II. General Comments

The Alliance applauds the Senator's initiative in discussing cybersecurity issues that are affecting the healthcare sector and seeking input from stakeholders on the challenges and opportunities. Indeed,

cybersecurity has become a serious threat to public health, not only in terms of the delivery of care services but also the significant impact on the costs, which have been rising continuously in the last few decades.

In particular, we are very concerned about the challenges posed by cybersecurity on medical devices, which are essential tools needed by the healthcare professionals to provide safe, high quality and cost-effective care to patients. This fact has been well proven during the COVID-19 pandemic.

We agree that the cybersecurity challenge requires significant effort and resources from both the public and private sectors. Your policy paper has described well the roles and responsibilities of the federal government and agencies, so we do not feel the need to add anything except to state that we fully agree that there is a clear need for a centralized leadership to coordinate those efforts to reduce risks of duplication and conflicts.

On the private sector side, we believe it is necessary to heighten the awareness of the critical role of the people and organizations who are responsible for the healthcare infrastructure, not only the Information Technology (IT) infrastructure but also the physical infrastructure such as the facilities (buildings and utilities) and the medical devices. More specifically, we are referring to the healthcare technology management (HTM) professionals who maintain, repair and manage medical devices deployed by HDOs. These professionals are employed by a variety of organizations, ranging from manufacturers (aka original equipment manufacturers - OEMs)—not only when servicing the devices they produced but also when servicing devices manufactured by other OEMs (aka multi-vendor service - MVS), HDOs themselves, and ISOs. Regardless of the nature of their respective employers, these HTM professionals have an important role in identifying cyber exploits and vulnerabilities and in participating in the prevention and mitigation efforts.

III. Specific Comments on the Policy Paper

Being among the largest medical device ISOs, we would like to provide the follow specific comments on your policy paper from our perspective. Our comments are provided below following the organization of your policy paper.

Section 2.2 - Addressing Insecure Legacy Systems

> *2. What sorts of requirements should medical devices have to meet in order to be eligible for reimbursement under a "cash for clunkers" style program? Does such an approach pose an unacceptable moral hazard?*
>
> We do not believe a "cash for clunkers" (after the 2009 Car Allowance Rebate System - CARS) style program is truly justified or cost effective. Our experience has shown that most medical equipment (i.e., a medical device that is capitalized because it is reusable and has exceeded a certain cost threshold) can be safely used well beyond the "useful life" or the "end of support/life" declared by the respective OEM. It is not unusual to find equipment with over 15-20 years of age within most HDOs, including some major teaching hospitals. As a matter of fact, as ISOs, we pride ourselves for being able to extend the useful life of medical equipment to save precious investment capital for our HDO clients.

Exhibit A provides a gross estimate of the cost to replace legacy devices currently deployed within HDOs. The amount of legacy devices is grossly estimated in the order of 2.4 – 5.5 million pieces and the replacement cost in the range of $30 - 70 billion. Prior to the pandemic, American community (non-governmental) hospitals as a whole were investing roughly $24 billion per year in medical equipment. The replacement of legacy devices would far exceed this value (by 123-286%). The HDO investment capability has obviously been severely reduced by the pandemic[1]. Even if a "cash for clunkers" style program were implemented, it is not clear that most HDOs can afford to advance the capital investment needed until the reimbursement is received.

Instead, we believe only a small fraction of such money is needed for OEMs to work with software companies to find suitable patches for most medical equipment alleged to be "insecure" by the respective OEMs. According to the FDA, it does not typically need to review such updates if they are solely for strengthening cybersecurity[2]. In parallel, we urge the Congress to consider ways to promote discussions between OEMs and HDOs (including their ISO partners) to establish a more gradual phasing out of these devices over a period of time that is feasible for the HDOs.

In addition, we encourage the Congress to consider providing some incentives for HDOs to implement tools to monitor and detect cybersecurity risks related to medical devices, such as early and favorable termination of audits and/or the mitigation of fines and penalties currently allowed by the HITECH Act in a security event when certain recognized security practices have been adopted.*3. Should providers have a "right to repair" medical equipment by contracting with third-party providers?*

While the "right to repair" (RtR) is an essential part of the effort to extend the useful life of equipment alleged to be "insecure" by the respective OEMs, it has very limited value. This is because FDA regulations (FD&C Act Section 501 and 21 CFR 820) prevent HTM professionals (regardless whether employed by HDOs, MVS or ISOs) from making alterations to the software embedded into medical devices, even if all OEMs provide technical specifications and software access per RtR. The only option is for HDOs to remove those legacy devices from their networks or isolate them into secure compartments (aka "segmentation") so they can control careful the data traffic.

On the other hand, RtR is an extremely valuable tool for HTM professionals (regardless employed by HDOs, MVS or ISOs) to be able to service both legacy and non-legacy equipment and ensure its cybersecurity protection, because it requires the OEMs to provide access to service materials (service manuals, proprietary tools and parts, access to diagnostic, repair and calibration software, and service training) at reasonable costs, thus allowing HDOs to select their own preferred service

[1] Beckers Hospital Review. More pain, no gain for hospitals' operating margins. Available at https://www.beckershospitalreview.com/finance/more-pain-no-gain-for-hospitals-operating-margins.html

[2] FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity. Available at https://www.fda.gov/media/103696/download

providers. Unfortunately, RtR is not yet a reality and some OEMs have adamantly refused to provide those service materials.

Even worse, some OEMs have already started to use the need to restrict software access (termed "privileged access" by the FDA[3]) to further limit the ability of HTM professionals to diagnose, repair and calibrate medical equipment, not only the legacy systems but also the non-legacy ones[4]. This will further reduce prompt access to healthcare services and almost surely raise the cost of healthcare.

4. Should medical equipment manufacturers be required to update their products for a certain length of time?

Currently medical device manufacturers are not required to provide maintenance services or parts for any length of time. Such requirement seems also absent from the Universal Commercial Code for consumer products. Therefore, any legislative action is likely to receive substantive rejection. In our view, the only option is for individual HDOs to specify the length of support, including cybersecurity software patches, in their acquisition contracts. Obviously, this only will be helpful for future acquisitions and not resolve the existing products.

IV. Conclusions

Again, the Alliance would like to commend Senator Warner and his staff for their efforts in addressing medical device cybersecurity.

As stated in the policy paper, this is an increasingly dangerous threat to public health and requires all stakeholders from both public and private sectors to collaborate to achieve the desired outcomes. A key component of the cybersecurity environment is the medical equipment deployed by HDOs and used by the medical professionals to provide care to the patients. Without safe and reliable medical equipment, it is not possible to deliver safe and high-quality care expected by the public, as well as control the financial burden placed on both public and private funds.

Therefore, we urge the Senator to lead the charge in the Congress to seek a common-sense solution that will allow Americans to continue enjoying superior care at reasonable cost, without risking their lives and wellbeing due to cyberattacks perpetuated by unscrupulous individuals and groups.

We remain interested and available to participate and contribute to securing medical devices against cyberattacks.

---

[3] FDA, Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities. Available at https://www.fda.gov/medical-devices/quality-and-compliance-medical-devices/discussion-paper-strengthening-cybersecurity-practices-associated-servicing-medical-devices

[4] Wang B. Is 'Privileged Access' the New 'License to Kill?' Available at https://24x7mag.com/standards/privileged-access-new-license-kill/

Sincerely yours,

The Alliance for Quality Medical Device Servicing

Exhibit A - Estimated Impact of Legacy Medical Equipment on HDOs

(NOTE: This estimation includes only capital medical devices, i.e., reusable devices with unit cost >$1,000)

DATA & ESTIMATES	VALUES	REFERENCES
A. Original Data and Respective Sources		
Total #staffed beds in community HDOs	787,995	[1]
Average #equipment per staffed bed	20	[2]
Average equipment cost/staffed bed ($M)	$0.25	[2]
Annual CapEx by community HDOs ($M)	$73,000	[3]
B. Calculated Values		
Total #medical equipment deployed in community HDOs	15,759,900	
Total equipment CapEx invested by community HDOs ($M)	$196,999	
C. Assumptions	**low estimate**	**high estimate**
Percentage of annual CapEx by HDOs on medical equipment	33%	
Percentage of legacy devices among existing equipment inventory	15%	35%
D. Estimated Impacts	**low estimate**	**high estimate**
Annual CapEx for medical equipment by community HDOs ($M)	$24,090	
Total number of legacy devices	2,363,985	5,515,965
Replacement cost of legacy devices ($M)	$29,550	$68,950
Replacement cost of legacy devices as a percentage of current annual CapEx (%)	123%	286%

References (Data Sources and Notes)

[1]	2021 AHA Hospital Statistics (https://www.aha.org/statistics/fast-facts-us-hospitals)
[2]	Wang B. Why maintenance cost to asset value ratio is not a good benchmark, Uptime, Aug-Sept 2018 (https://reliabilityweb.com/articles/entry/why-maintenance-cost-to-asset-value-ratio-is-not-a-good-benchmark). The original value of 18 equipment/bed and $200k/bed were adjusted to 20 and $250k to reflect healthcare inflation from 2013 to 2021.
[3]	Definitive Healthcare (https://www.definitivehc.com/data-products/hospital-view)

Exhibit B - Estimated Impact of Privileged Access on Medical Equipment

(NOTE: This estimation includes only capital medical devices, i.e., reusable devices with unit cost >$1,000)

DATA & ESTIMATES	VALUES	REFERENCES
A. Original Data and Respective Sources		
Total operating expenses for community HDOs ($M)	$1,056,497	[1]
% of total HDO expenses spent on medical equipment service	1%	[2]
Total #staffed beds in community HDOs	787,995	[1]
Average equipment cost/staffed bed ($M)	$0.25	[2]
Annual capital investment by community HDOs ($M)	$73,000	[3]
B. Calculated Values		
Total equipment CapEx invested by community HDOs ($M)	$196,999	
Total medical equipment servicing costs in community HDOs ($M)	$10,565	
C. Assumptions for OpEx Estimation		
Current OEM service market share of medical equipment services	50%	
OEM service market share **if** service is mostly limited to OEM by "privileged-access"	90%	
OEM service cost premium (% above HDO or ISO cost)	75%	
D. Estimated Impact on OpEx		
Additional costs for HDOs in medical equipment servicing **if** service is mostly limited to OEM by "privileged-access" ($M)	$3,169	
E. Assumptions for CapEx Estimation		
Average daily equipment available time (hours)	12	
Current average annual equipment downtime (hours)	20	
Increase in equipment annual downtime **if** service is mostly limited to OEM by "privileged-access" (hours)	36	
Decrease in equipment lifecycle forced by OEM by "privileged-access" (from 10 years to 6.5 years)	54%	
Percentage of annual CapEx spent on medical equipment by community HDOs	33%	
F. Estimated CapEx Values		
Current annual equipment CapEx by community HDOs ($M)	$24,090	
Increase in CapEx needed to compensate for higher downtime ($M)	$1,627	
Increase in **annual** CapEx needed to compensate for shortened useful lifecycle ($M)	$12,972	

References (Data Sources and Notes)

[1] 2021 AHA Hospital Statistics (https://www.aha.org/statistics/fast-facts-us-hospitals)

[2] Wang B. Why maintenance cost to asset value ratio is not a good benchmark, Uptime, Aug-Sept 2018 (https://reliabilityweb.com/articles/entry/why-maintenance-cost-to-asset-value-ratio-is-not-a-good-benchmark). The original value of 18 equipment/bed and $200k/bed were adjusted to 20 and $250k to reflect healthcare inflation from 2013 to 2021.

[3] Definitive Healthcare (https://www.definitivehc.com/data-products/hospital-view)