ALLIANCE
FOR QUALITY MEDICAL DEVICE SERVICING

Cybersecurity is a critical issue impacting all industries and none more than healthcare, which remains the most attacked critical infrastructure in the nation. From 2021 to 2022, cyberattacks on healthcare delivery organizations (HDOs) increased 86% from 758 attacks per week to 1,410[1]. Additionally, 53% of medical devices have known critical vulnerabilities[2], and for the past 12 years HDOs have the highest cost per breach at +$10M with a record number of breaches in 2021[3]. Nearly one quarter of surveyed HDOs stated cyberattack victims experienced increased mortality rates following a data breach, and more than half reported inferior patient outcomes due to longer hospital stays and delayed procedures[4]. At its core cybersecurity in healthcare is a patient safety issue.

The Alliance for Quality Medical Device Servicing applauds the inclusion of cybersecurity requirements in the recent omnibus bill (H.R.2617 - Consolidated Appropriations Act, 2023). We support the requirement for the Original Equipment Manufacturers (OEMs) to address cybersecurity in premarket submissions and provide a plan to address post-market issues. There are currently about 2.4 – 5.5 million medical devices in use with possible vulnerabilities to cyberattacks ("legacy devices"). These devices are working well and are essential for the care of patients in almost all HDOs, "particularly in rural and underserved communities" as stated by FDA. It is not feasible to follow the "quick fix" to the cybersecurity issue of simply replacing these legacy devices as advocated by some groups because HDOs don't have the $30 - 70B capital needed (prior to the COVID-19 pandemic, all American community (non-governmental) hospitals were only able to spend ~$24B/year), and the OEMs are also unlikely able to produce such a large number of devices due to supply chain challenges[5].

Considering the above, it is imperative firm and prompt actions are taken in these areas to ensure patient safety:

- **Access:** to service information, materials, and diagnostic/calibration software not only to enable prompt maintenance but also detection of new vulnerabilities.
- **Reporting:** of new vulnerabilities by HDOs, device users and servicers to a centralized organization all users and servicers can easily access.
- **Remediation:** through validated patches and mitigations for known vulnerabilities, particularly for the millions of legacy devices.

Access by medical devices servicers to service information, materials and diagnostic/calibration software is necessary to address vulnerabilities and keep devices safe. Some OEMs and associated groups are advocating for restricted access to device diagnostic/calibration software ("privileged access") and service materials claiming that this will increase cyber-risks, although there is no data to support these claims. Without such access, it will not only be impossible to participate and assist in the cybersecurity efforts but also severely limit servicers' ability to maintain devices. This could lead to not only unsafe and out of specification devices but also to delays in care, putting patients' lives at additional risk.

Currently, there is no single organization that is systematically collecting and testing new cyber vulnerabilities. HDOs and their servicers should be able to report all suspicious cyber vulnerabilities for evaluation by subject matter experts.

Once confirmed, the respective OEM should be notified and given a timeframe for remediation. Today, many of the known medical device vulnerabilities are not being resolved by the OEM in a timely manner, if at all, by either providing a patch or compensating control. This is clearly a significant public health risk.

Medical device cybersecurity is critical to patient safety and is a core component of an effective and safe service strategy. Ensuring servicers have access to device diagnostic/calibration software, service tools and materials, and training, as well as requiring OEMs provide validated patches and support legacy devices in a timely manner is critical. We urge Congress and relevant agencies to take decisive action to address cybersecurity for medical devices.

****

The Alliance for Quality Medical Device Servicing was formed in 2018 and is comprised of five leading national medical device service organizations: TRIMEDX, Sodexo, Crothall, Agiliti, and the InterMed Group. Alliance members collectively employ tens of thousands of technicians, clinical engineers and skilled professionals who provide medical device repair and servicing in hospitals and health systems in all 50 states.

[1] https://www.insiderintelligence.com/content/healthcare-cybersecurity-2023-hive-s-shutdown-good-news-cyberattacks-only-getting-worse
[2] Critical Medical Device Risks Continue to Threaten Hospital Security
[3] https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ https://www.ibm.com/security/data-breach
[4] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf
[5] https://24x7mag.com/standards/privileged-w-license-kill/