Recommendations for Medical Device Cybersecurity Terms and Conditions

The Healthcare Supply Chain Association has circulated “Medical Device and Service Cybersecurity: Key Considerations for Manufacturers & Healthcare Delivery Organizations (HDOs)” which outlines the shared responsibilities of the parties in assuring medical device and information security and some of the steps they might take in promoting that security. We believe that suppliers should view the rapid adoption of rigorous cybersecurity measures and compliance with published guidelines as a necessary precondition to marketing medical devices

In support of these key considerations, we recommend that purchasing contracts include clauses reflective of the following principles for the acquisition of connected medical devices and services:

1) Suppliers should **warrant their compliance with FDA premarket and post-market guidance** relative to cybersecurity risks throughout their product’s lifecycle.

2) Products should be **assessed and warranted to be free of known malware or other vulnerabilities** at the time of delivery, and/or implementation, and throughout the life of the product.

3) Suppliers should **comply with all reasonable security practices required by the HDO** that are consistent with current network and device security guidelines and best practices including those developed and implemented by the HDO, the Federal Information Security Management Act (FISMA) or as published by standards bodies such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Association for the Advancement of Medical Instrumentation (AAMI), the Open Web Application Security Project (OWASP), the SANS Institute, the Center for Internet Security, the National Institute of Standards and Technology (NIST).

4) The expected useful life of the device or service should be **specified within the purchase agreement** and security updates to the software, operating system and all supporting software components should be made available for the stated useful life at no additional cost to the HDO. This is to include, but not be limited to, monitoring, upgrading, updating, and patching in a manner consistent with the HDO’s protocols.

5) Suppliers should make every effort to **assist HDOs in resolving cybersecurity threats and vulnerabilities in a timely manner**. This includes, but is not limited to, providing timely updates and patches, a portal for sharing vulnerability information, and a security contact. HDOs should not be penalized by supplier for defects caused by modifications made to products in HDOs’ remediation efforts if the supplier fails to provide timely updates and/or timely assistance in addressing cybersecurity threats and vulnerabilities involving supplier’s products.

6) Purchase agreements and/or information security agreements for medical devices and services should **contain appropriate liability and warranty provisions** in regards to compliance with cybersecurity terms.

7) HDOs’ participation in Information Sharing and Analysis Organizations (ISAOs) and other cyber security sharing initiatives **should be explicitly allowed and exempted from any non-disclosure provisions**.

Contract terms should require that manufacturers/suppliers provide documentation as follows:

8) The most current version of the Manufacturers Disclosure Statement for Medical Device Security (MDS2) **must be provided for any device that maintains or transmits protected health information** (PHI) and/or personally identifiable information (PII).

9) Suppliers should **warrant that they internally follow cybersecurity best practices such as ISO 27001, SOC II or their equivalents approved by the HDO**, provide documentation describing in detail their cybersecurity/penetration testing and risk assessment processes as well as program details for patching, incident response and secure set up and configuration

10) Suppliers should **utilize an industry recognized vulnerability scoring methodology** such as the Common Vulnerability Scoring System (CVSS) and must disclose that methodology along with processes, procedures, resources and timelines for communicating and addressing identified vulnerabilities and threats.

11) Suppliers must **provide documentation of processes and technology for external access and remote support**, including security (authentication & authorization) and monitoring.

12) Suppliers/manufacturers should **warrant ongoing and active participation in one or more Information Sharing and Analysis Organizations** (ISAO) and provide their vulnerability disclosure protocols.

13) A bill of materials describing the component parts of products including a Software Bill of Materials (SBoM) should be **provided to the HDO prior to implementation** which includes software versions, patch levels, and patching plans. The product lifecycle/expectancy should be explicitly stated.

14) Supplier should **provide a product roadmap depicting the lifecycle of the product** including end of service, end of life, and end of support.