Recommendations for Medical Device Cybersecurity Terms and Conditions

HSCA
HEALTHCARE SUPPLY CHAIN ASSOCIATION
Innovators In Evidence-Based Sourcing

The Healthcare Supply Chain Association has circulated "Medical Device and Service Cybersecurity: Key Considerations for Manufacturers & Healthcare Providers" 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 an opportunity to develop competitive advantage.

In support of these key considerations, we recommend that purchasing contracts include clauses reflecting 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 malicious code or other vulnerabilities at the time of delivery and/or implementation.

3) Suppliers should comply with all reasonable security practices required by the provider that are consistent with current network and device security guidelines and best practices including those developed and implemented by the provider or as published by standards bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission(IEC) (ISO/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 and 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 and all supporting software components should be made available for the stated useful life at no additional cost to the provider. This is to include monitoring, upgrading and patching in a manner consistent with the provider's protocols.

5) Suppliers should make every effort to assist providers in resolving cybersecurity threats and vulnerabilities in a timely manner. Providers should not be penalized for defects caused by modifications made to products in remediation efforts if the supplier fails to provide such assistance.

6) Purchase agreements for medical devices and services should contain appropriate liability and warranty provisions that contain no limitations on supplier's liability due to failure to comply with cyber security terms.

7) Providers participation in ISAOs and other cyber security sharing initiatives should be explicitly allowed and exempted from any non-disclosure provisions.

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

8) A Manufacturers Disclosure Statement for Medical Device Security (MDS2) should be provided for any device that maintains or transmits data.

9) Suppliers should warrant that they internally follow cybersecurity best practices, provide documentation describing in detail their cybersecurity/penetration testing process as well as program details for patching, incident response and secure set up and configuration.

10) Suppliers should provide documentation of processes and technology for external access, including security (authentication & authorization) and monitoring.

11) Suppliers/manufacturers should warrant ongoing and active participation in one or more Information Sharing and Analysis Organization (ISAO), provide a certificate of participation and provide their vulnerability disclosure protocols.

12) A bill of materials describing the component parts of products including software should be provided to the provider prior to implementation that includes software versions, patch levels, and patching plans. The product lifecycle/expectancy should be explicitly stated.