Medical Device Security and Responsible Vulnerability Disclosure

1. Medical Device Security Standards
   a. Medical Devices in the scope of this agreement that are required to meet IU Health Security Standards include devices that have:
      i. Serial (RS-232, RS-485, etc.), Ethernet, Wireless Ethernet, Bluetooth, ZigBee, Cellular data, or other technologies that allow the wired or wireless transmission of data or signals over radio frequencies to another device or computer.
      ii. Persistent storage on the device itself such as a hard drive, solid state disk (SSD), or flash memory.
      iii. Universal Serial Bus (USB) ports.
      iv. Secure Digital (SD) or other forms of removable storage.
      v. A Central Processing Unit (CPU) and Random Access Memory (RAM) used for performing its essential functions.
      vi. A computing device attached to assist the device in performing its intended function.
   b. Applicable devices need to meet the requirements stipulated in the IU Health Standard Information Security Requirements and Demonstration of Compliance exhibit.
   c. Additionally, applicable devices need to demonstrate compliance with either the FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices guidance, and/or the Underwriters Laboratories (UL) Standards for Software Cybersecurity for Network-Connectable Products (UL 2900-1).

2. Responsible Vulnerability Disclosure Policy
   a. Vendor hereby agrees to permit Indiana University Health (“IU Health”) and its subcontractors to conduct product and application security testing of devices in the scope of this agreement without limitation or restrictions and with the intent to identify potential security vulnerabilities in the software, hardware, devices, antennae, related configurations, and other properties available (“potential vulnerabilities”) on the devices in scope of this agreement.
   b. IU Health agrees equipment upon which any security testing is performed will not be placed in patient care operations. IU Health agrees to disclose potential vulnerabilities to Vendor at no unreasonable day and within 90 days of IU Health identification.
   c. Vendor agrees to provide a vulnerability mitigation plan to IU Health within 7 days of report and make product enhancements available within 90 days should IU Health, according to its own definition, determine the vulnerability prevents safe device utilization.
   d. Furthermore, Vendor agrees to publicly disclose potential vulnerabilities as soon as reasonably possible and at least within 90 days of receipt from IU Health.

3. Medical Device Security Incident Costs
   a. In the event of a Security Incident which Covered Entity or other entity with Privacy and Security Rules enforcement jurisdiction determines was proximately caused by nonconformance with the terms and conditions described in Indiana University Health, Inc. Standard Information Security Requirements and Demonstration of Compliance, Business Associate shall be responsible for all costs associated with the incident, including but not limited to: (i) Updating of device firmware and software to mitigate the vulnerability which caused the Security Incident to a current, non-vulnerable version; (ii) Updating of software on associated computing devices, servers, and supporting technology infrastructures to current, non-vulnerable versions; (iii) Remuneration for time spent by internal or contracted IU Health resources to mitigate the vulnerability; (iv) Reconfiguration of the Medical Device environment to conform to the Terms and Conditions in the Security Exhibit; (v) Retesting of the environment by IU Health Information Security or a third party to verify and validate that the Medical Device environment conforms to the requirements of the Standard Information Security Requirements and Demonstration of Compliance exhibit.