Memorandum of Agreement

Between

The Department of Homeland Security,
National Protection and Programs Directorate
And

The Department of Health and Human Services,
Food and Drug Administration

Relating to

Medical Device Cybersecurity Collaboration

I. **Parties**. This Memorandum of Agreement (Agreement) is entered into between the United States Department of Health and Human Services (HHS), Food and Drug Administration (FDA) (hereinafter FDA) and the United States Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), collectively, "the Parties."

II. **Purpose.** This Agreement is executed to formalize and enhance the working relationship of the Parties, including roles and responsibilities, when sharing information related to vulnerabilities and threats to the Healthcare and Public Health that involve the cybersecurity of a medical device(s). The goal is to share such information to enhance mutual awareness, heighten coordination, catalyze standards development, and enhance technical capabilities between the Parties. This Agreement provides a framework for coordination and the principles and procedures by which information sharing and related interactions between the Parties shall take place.

This Agreement also establishes a foundation by which NPPDcan support FDA as an independent third-party for technical analysis and testing.

III. **Authority**. This Agreement is concluded pursuant to authorities applicable to the Parties, including:

- The Homeland Security Act of 2002, Pub. L. 107-296. 116 Stat. 2135 (2002), as amended. See esp. § 227.
- The Federal Food, Drug, and Cosmetic Act ("FD&C Act"), 21 U.S.C. § 301 *et seq.* and its implementing regulations.

IV. Definitions.

A. Device: an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is—(1) recognized in the official National Formulary, or the United States

Pharmacopeia, or any supplement to them, (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 360j(o) of this title. (21 U.S.C. § 321(h)).

B. Confidential Commercial Information ("CCI"): valuable data or information which is used in a business and is of such type that it is customarily held in strict confidence or regarded as privileged and not disclosed to any member of the public by the entity to whom it belongs. Examples of CCI include raw material supplier lists, finished product customer lists, traceback information, etc. (21 C.F.R. § 20.61).

C. Protected Critical Infrastructure Information ("PCII"): validated Critical Infrastructure Information as defined in Federal Regulation at 6 CFR 29.2(g).

D. Medical Device Manufacturer: any person who designs, manufactures, fabricates, assembles, or processes a finished device. Manufacturer includes but is not limited to those who perform the functions of contract sterilization, installation, relabeling, remanufacturing, repacking, or specification development, and initial distributors of foreign entities performing these functions. (21 C.F.R. § 820.3(o)).

E. Non-public Information: includes, but is not limited to, CCI, Trade Secret Information, and PCII.

F. Trade Secret Information: any commercially valuable plan, formula, process or device that is used for making, preparing, compounding, or processing of trade commodities, that can be said to be the end product of either innovation or substantial efforts. In order for proprietary information to be considered a trade secret, there must be a direct relationship between the trade secret and the production process. (21 C.F.R. § 20.61).

V. **Background**. The Department of Homeland Security's missions include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience. Information-sharing is a key part of the DHS mission to create shared situational awareness of malicious cyber activity. Cyberspace has united once distinct information structures, including business and government operations, emergency preparedness communications, and critical digital and process control systems and infrastructures. Protection of these systems is essential to the resilience and reliability of the nation's critical infrastructure and key resources; therefore, to economic and national security.

The National Protection and Programs Directorate leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. NPPD works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services.

The FDA promotes and protects the public health by ensuring the safety, efficacy, and security of drugs, biological products, veterinary products, medical devices and radiological products and the safety and security of foods and cosmetics. The FDA administers the FD&C Act (see generally, 21 U.S.C. § 301 et. seq.) and certain sections of the Public Health Service Act (see, e.g., 42 U.S.C. § 262), among other statutes. Among its duties, the FDA approves pre-market applications for medical products, conducts inspections of manufacturing facilities, and monitors post-marketing adverse events. The FDA also initiates civil and criminal litigation to enforce applicable laws and regulations.

The FDA's Center for Devices and Radiological Health (CDRH) is responsible for ensuring that patients and healthcare providers have access to safe and effective medical devices. To advance patient care, medical devices are becoming increasingly interconnected and interoperable. However, interconnected devices also increase cybersecurity risks which, if exploited, may affect device performance. CDRH is committed to enhancing patient safety by mitigating cybersecurity risk throughout the life cycle of medical devices. This includes monitoring, identifying, and addressing cybersecurity vulnerabilities in medical devices once they are on the market. CDRH works collaboratively with industry, healthcare organizations, and government entities to address cybersecurity risks to medical devices.

VI. **General Provisions**. This is a collaborative agreement between the Parties regarding sharing of information related to vulnerabilities and threats to the Healthcare and Public Health Sector that involve the cybersecurity of a medical device(s).[1]

The Parties jointly agree to cooperate and share information, to the extent possible, as follows:

A. NPPD and FDA should collaborate to mutually enhance awareness of medical device cybersecurity vulnerabilities and threats to the Healthcare and Public Health sector, but not in a capacity that interferes with any other roles and responsibilities of the parties.

B. NPPD, through the National Cybersecurity and Communications Integration Center (NCCIC), functions as a trusted collaborator among researchers, manufacturers, and other governmental entities, consistent with NCCIC's broad cybersecurity risk information receipt, analysis, and sharing authorities. Given this role, NCCIC will coordinate and enable information sharing between medical device manufacturers, researchers, and the

[1] The provisions of this agreement are not intended to add to or detract from any of the authorities of either FDA or NPPD. Each party reserves the authority to review, independently from the other, matters of concern under their respective authorities.

FDA's Center for Devices and Radiological Health, particularly in the event of cybersecurity vulnerabilities in medical devices identified to NPPD.

C. Should cooperation under this MOA identify opportunities for the Parties to better coordinate activities through joint action (e.g., coordinated assignment of Common Vulnerabilities and Exposures (CVE) identifiers for health care system vulnerabilities) the Parties should pursue and formalize such collaboration/coordination.

D. If the parties agree that there is a need, NPPD can support FDA as an independent third-party to aid in the evaluation and assessment of the impact of medical device vulnerabilities, subject to availability of DHS resources and funding or a separate Interagency Agreement document between the FDA and NPPD.

VII. **Responsibilities**. As part of this collaborative agreement the Parties agree to the following responsibilities.

A. NPPD Responsibilities

1. Serve as central medical device vulnerability coordination center and interface with appropriate stakeholders in performance of such duties, consistent with current NCCIC policies and procedures.

2. Participate in regular, ad hoc, and emergency coordination calls with FDA to enhance mutual awareness of medical device cybersecurity vulnerabilities and threats to the Healthcare and Public Health sector and device manufacturers operating within that sector.

3. Confer with entities providing sensitive information regarding medical devices prior to sharing any CCI, trade secret, or PCII-protected vulnerability or product information with the FDA. Following approval to share information, NPPD will notify the FDA of cybersecurity vulnerabilities in medical systems and related information that have been reported to NPPD.

4. Coordinate with FDA on the content of alerts and advisories related to medical device cybersecurity to be published by DHS.

5. Maintain technical capabilities to support requests for independent third-party analysis to aid in the evaluation and assessment of the impact of medical device vulnerabilities, which can be used upon the agreement of both parties.

6. Publish Healthcare and Public Health related alerts and advisories, including those related to specific medical devices, to the National Health Information Sharing and Analysis Center (NH-ISAC) to raise stakeholder awareness of vulnerabilities and mitigations. Such alerts and advisories will not be exclusively provided to the NH-ISAC.

B. FDA Responsibilities

1. Coordinate and participate in regular, ad hoc, and emergency coordination calls with NPPD to enhance mutual awareness of medical device cybersecurity vulnerabilities and threats to the Healthcare and Public sector and to facilitate resolutions to vulnerability coordination issues.

2. Provide NPPD with draft public releases, when possible, for review to facilitate coordination of messaging among Federal entities.

3. Comment in a timely manner on NPPD draft advisories and alerts to facilitate consistent public messaging between the Parties.

4. Make assessments regarding the risk to health and the risk of patient harm when the potential impact of a medical device cybersecurity vulnerability is disputed.

5. Submit requests to NPPD for independent third-party technical assistance to analyze and test medical systems, as appropriate.

6. Shares non-trade secret information with NPPD, consistent with applicable laws (e.g. 21 U.S.C. 360j(c)), that is necessary to resolve disputes of risk, impacts, and communication alignment

VIII. Information Sharing.

1. The Parties recognize that exchanged information may contain any of the following types of information and as such must be protected from unauthorized use and disclosure:

   A. CCI and/or Trade Secret Information, such as the information that would be protected from public disclosure pursuant to Exemption 4 of the Freedom of Information Act ("FOIA") (5 U.S.C. § 552);
   B. Personal privacy information, such as the information that would be protected from public disclosure pursuant to Exemption 6 or 7(C) of the FOIA; or
   C. Information that is otherwise protected from public disclosure by Federal laws and their implementing regulations (e.g., Trade Secrets Act (18 U.S.C. § 1905), the Privacy Act (5 U.S.C. § 552a), other FOIA exemptions not mentioned above (5 U.S.C. § 552(b)), the FD&C Act (21 U.S.C. § 301 *et seq.*), and the Health Insurance Portability and Accountability Act ("HIPAA"), (Pub. L. 104-191)).

2. The Parties recognize and acknowledge that it is essential that any non-public information that is shared between the Parties, whether written or oral, cannot be further shared unless authorized by law. *See e.g.,* 21 U.S.C. § 331(j), 21 U.S.C. § 360j(c), 18 U.S.C. § 1905, 21 CFR Parts 20 and 21. In some cases, such information also cannot be further shared unless specifically authorized by and with the consent of the original information provider. Any non-public information shared under this MOA will not be further disclosed without the

written permission of the originating agency.

3. Pursuant to section 301(j) of the FD&C Act (21 USC §§ 331(j)), FDA will not disclose certain trade secret information to NPPD. Pursuant to section 520(c) of the FD&C Act (21 U.S.C. § 331j(c)), certain CCI could be disclosed to "officers and employees concerned with carrying out [the] Act or when relevant in any proceeding under [the Act]." 21 U.S.C. §360j(c).

4. Within 90 days of the execution of this Agreement, the NCCIC and CDRH will develop a standard operating procedure for information sharing and exchange pursuant to this MOA.

5. The Participants will establish proper safeguards to ensure that non-public information shared under this MOA will be used and disclosed solely in accordance with applicable laws and regulations.

    a. Proper safeguards will include the adoption of policies and procedures to ensure that the information shared under this MOA will be shared and used consistent with the Trade Secrets Act (18 U.S.C. § 1905), the FD&C Act (21 U.S.C. § 301 *et seq.*), the Privacy Act of 1974, (5 U.S.C. § 552a), the Freedom of Information Act (5 U.S.C. § 552), the Critical Infrastructure Information Act, (6 U.S.C. § 133), the confidentiality or non-disclosure provisions of any other agreement entered into by NPPD or FDA, and other applicable Federal laws and their implementing regulations.

    b. Proper safeguards will protect against unauthorized use and disclosure of the non-public information shared or exchanged pursuant to this MOA and such safeguards are necessary for effective implementation of this MOA.

    c. Access to the information shared or exchanged under this MOA will be restricted to authorized Parties' employees, agents, contractors, and officials who require access to perform their official duties in accordance with the uses of information as authorized by this MOA and the authorities of the Parties. Such personnel will be advised of: (1) the confidential nature of the information; (2) safeguards required to protect the information; and (3) the administrative, civil, and criminal penalties for noncompliance contained in applicable Federal laws. Contractors, their subcontractors, and agents requiring access to the non-public information shared or exchanged under this agreement must be covered by an agreement that requires them to keep the information confidential.

    d. The Parties agree to notify promptly each other of any actual or suspected unauthorized disclosure of any information shared pursuant to this MOA.

    e. The Agency who has received shared information (requesting Agency) will promptly notify the contact person or designee of the sharing Agency of any attempt by a third party to obtain shared non-public information by compulsory process, including, but not limited to, a FOIA request, subpoena, discovery request, or litigation complaint or

motion.

f. If an Agency that has received information under this MOA receives a FOIA request where there are responsive records which originated with the other Agency, this Agency will refer the FOIA request to the other Agency for it to respond directly to the FOIA requestor. In such cases, the Agency, which received the FOIA request will notify the FOIA requestor that it has referred the FOIA request to another Agency and that a response will issue directly from that Agency.

g. The requesting Agency will notify the sharing Agency before complying with any judicial order that compels the release of shared non-public information, so that the Parties may determine the appropriate measures to take, including, where appropriate, legal action.

IX. Points of Contact.

John Felker
National Cybersecurity and Communications Integration Center
U.S. Department of Homeland Security
703-235-8864
john.felker@hq.dhs.gov

Suzanne B. Schwartz, MD, MBA
Associate Director for Science and Strategic Partnerships
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Avenue
Building 66, Room 5434
Silver Spring, MD 20993
301-796-6937
suzanne.schwartz@fda.hhs.gov

Seth Carmody, PhD
Senior Project Manager for Cybersecurity
Emergency Preparedness/Operations and Medical Countermeasures (EMCM) Program
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Avenue
Building 66, Room 4652
301-796-6944
seth.carmody@fda.hhs.gov

X. **Other Provisions**. Nothing in this Agreement is intended to conflict with current law. If a term of this Agreement is inconsistent with any applicable law, then that term will be invalid, but the remaining terms and conditions of this Agreement will remain in full force and effect.

XI. **Resource Obligations**. This Agreement represents the broad outline of the Parties' intent to enter into collaborative efforts in areas of mutual interest to the Parties. All activities undertaken pursuant to this Agreement are subject to the availability of personnel, resources, and funds. This Agreement does not affect or supersede any existing or future agreements or arrangements between the Parties and does not serve to commit or obligate any funding or resources of the Parties. This Agreement does not create binding, enforceable obligations against the Parties. This Agreement and all associated agreements will be subject to the applicable policies, rules, regulations, and statutes under which the Parties operate

XII. **Effective Date**. This Agreement is effective on the date of the final signature.

XIII. **Modification**. The Parties may modify this Agreement by written agreement, signed by authorized representatives of both Parties.

XIV. **Termination**. Either Party may terminate this Agreement at any time by providing at least 30 calendar days' written notice.

XV. **Costs**. This Agreement does not obligate any funds. Each party shall remain responsible for its own costs to perform its responsibilities under this Agreement. All responsibilities herein are subject to the continued availability of funds.

XVI. **Dispute Resolution**. The Parties will make their best efforts to amicably resolve disputes that may arise under this Agreement through discussions. If resolution cannot be reached, the Parties will solicit the views and mediation of the above referenced technical points of contact. If those views or mediation cannot be obtained, or fail to resolve the matter, the issue will be elevated through the respective signatories to this Agreement for resolution.

Approved By:

Food and Drug Administration

Scott Gottlieb, M.D.
Commissioner

Date: 10/15/18

Department of Homeland Security

Christopher C. Krebs
Under Secretary
National Protection and Programs Directorate

Date: 10/12/18