NCHICA

April 8, 2016

Docket ID:	FDA-2015-D-5105
Agency:	Food and Drug Administration (FDA)
Parent Agency:	Department of Health and Human Services (HHS)
Summary:	Draft Guidance for Industry and Food and Drug Administration Staff

Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Room 1061
Rockville, MD 20852

Subject: Postmarket Management of Cybersecurity in Medical Devices

To Whom It May Concern:

The North Carolina Healthcare Information and Communications Alliance (NCHICA) is a non-profit organization dedicated to accelerating the transformation of the U.S. healthcare system through the effective use of information technology, informatics and analytics. NCHICA's membership consists of a broad range of stakeholders in healthcare including providers, academic medical centers, vendors, governmental bodies, health plans, and research organizations. NCHICA has been active in the area of information privacy and security since 1994.

We applaud the FDA's efforts to increase the security of medical devices. However, we believe that the current guidance document can be improved. Our recommendations are as follows:

1. Recommendation vs. Requirement
   We understand that the current draft document is not a mandated standard; however, we see great value in setting a timeline for when this will be a requirement. Unfortunately, most companies will not follow this if it is only a recommendation.

2. Penalties
   As this document is a recommendation, not a requirement, a penalty for not addressing security issues was never discussed. Many companies ignored the HIPAA compliance guidelines until fines were levied on non-compliant organizations. Options are:
   - Loss of FDA Certification
   - Fines

3. Public Disclosure of Non-compliant Manufacturers
   HHS currently lists breaches of 500 or more records (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf). The same type of website could be created for medical device manufacturers who do not comply.

North Carolina Healthcare Information and Communications Alliance, Inc.
PO Box 13048, Research Triangle Park, NC 27709-3048 www.nchica.org

NCHICA

4. Reporting Non-compliant Manufacturers
   Update the Medwatch website to allow organizations and individuals to report non-compliant medical device manufacturers. Allow anonymous reporting of security issues. https://www.accessdata.fda.gov/scripts/medwatch/index.cfm?action=reporting.home

5. Eliminating Non-Supported Software
   While compensating controls are important for vulnerable devices in the field, medical device manufacturers should not be allowed to use non-supported operating systems and software in new device deployments. When a sunset has been announced, net-new deployments with the old operating system should not be allowed.

6. Availability/Load Testing
   Make the devices more robust so owners can perform internal security testing without the device crashing. Confidentiality, Integrity, and Availability are the core pillars of security.

7. System Hardening
   Devices should adhere to system hardening best practices. Many medical device vendors state that antivirus cannot be installed on their system even though they are running a standard Windows operating system.

8. Vulnerability Reporting Requirements
   The circumstances (lines 581-590) that allow for not reporting a vulnerability under 21 CFR part 806 are rather broad and do not necessarily ensure effective dissemination of the information. A separate reporting requirement specifically for cybersecurity-related vulnerabilities and their fixes could be more effective and could also be developed into a searchable reference for the customer base and user community.

NCHICA would be pleased to work with the appropriate parties in the FDA to address the issues at hand and to cooperate with the FDA in improving security in medical devices.

Thank you for your consideration of our concerns. Questions or comments may be directed to NCHICA.

Sincerely,

Jennifer Anderson
Executive Director

On behalf of the NCHICA Privacy, Security, and Technology Workgroups
Jon Sternstein, Principal Consultant, Stern Security
Todd Green, GRC Manager, Carolinas HealthCare System
Justin Tuck, Security & Privacy Analyst, Lenoir Memorial Hospital
Tom Schnittker, ISD Manager, UNC Health Care System

North Carolina Healthcare Information and Communications Alliance, Inc.
PO Box 13048, Research Triangle Park, NC 27709-3048 www.nchica.org