3108 Fifth Avenue
Suite B
San Diego, CA 92103
WorldPrivacyForum.org

Comments of World Privacy Forum to the Food and Drug Administration regarding Postmarket Management of Cybersecurity in Medical Devices. Docket No. FDA-2015-D-5105

Via Regulations.gov

Office of the Center Director,
Guidance and Policy Development
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Ave., Bldg. 66, Rm. 5431
Silver Spring, MD 20993-0002

April 4, 2016

The World Privacy Forum welcomes this opportunity to submit comments on the Food and Drug Administration's Draft Guidance on Postmarket Management of Cybersecurity in Medical Devices. The draft guidance appeared in the January 22, 2016, Federal Register (81 Fed. Reg. 3803) at https://www.gpo.gov/fdsys/pkg/FR-2016-01-22/pdf/2016-01172.pdf.

The World Privacy Forum is a non-profit public interest research and consumer education group. We publish original research papers and policy comments focused on privacy and security issues. We have testified before Congress multiple times, and many federal agencies. Much of our work explores technology and health-related privacy issues, biometrics, consent, data analytics, and many other rapidly evolving areas of privacy. We have testified before the FDA at its workshops, and issued reports regarding other FDA programs, with good results.[1] You can see our publications and find more information at www.worldprivacyforum.org.

[1] **Statement of the World Privacy Forum at the FDA/AHRQ Public Workshop, *Implementation of Risk Minimization Action Plans to Support Quality Use of Pharmaceuticals: Opportunities and Challenges,*** http://www.worldprivacyforum.org/wp-content/uploads/2007/06/WPF_RiskMAP_FDA28June2007fs.pdf, and **Written statement of Pam Dixon before the FDA Dermatologic and Ophthalmic Drugs Advisory**

I. General Comments

The World Privacy Forum welcomes the FDA's attention to the cybersecurity of medical devices. We agree that both the rapidly evolving Internet of Things and the Internet of Bodies present increasing threats to privacy and security from many types of technologies. The ongoing proliferation of cyber medical devices also presents challenges to regulators to keep pace with both the technology of the devices and with the demands (both legal and illegal) for personally identifiable information (PII) produced by the devices.

Our research into devices, sensors, and mesh networks has led us to understand that one of the problematic issues with medical devices is that people who mean well may unwittingly be using systems that are inherently unsecured. They may not intend to leak identifiable health data, and they may not even know they have leaked data. But device-based systems and networks can be insecure, nonetheless.

Personally identifiable health data is valuable to many, both on the legal and illegal side of data acquisition. It is now unambiguously documented that data brokers want to acquire health-related data that is identifiable in meaningful ways.[2] And the collection can be perfectly legal in many contexts. Beyond this risk, we have all become aware of the threat of health data breaches from determined hackers who steal the data with malicious intent.

Given the threat landscape, we are broadly supportive of the goals of the draft guidance. Specifically, we welcome these statements from the FDA:

> [M]anufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. (Line 17).
>
> This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. (Line 28)
>
> Cybersecurity risk management is a shared responsibility among stakeholders including, the medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA. FDA seeks to encourage collaboration among stakeholders by clarifying, for those stakeholders it regulates,

---

Committee and the Drug Safety and Risk Management Advisory Committee Regarding Privacy and the iPledge Program, http://www.worldprivacyforum.org/wp-content/uploads/2009/03/WPF_FDAiPledge_08012007fs.pdf.

[2] Silverman, Rachel Emma, *Bosses Harness Big Data to Predict Which Workers Might Get Sick*, Wall Street Journal, Feb. 16 2016, http://www.nasdaq.com/article/bosses-harness-big-data-to-predict-which-workers-might-get-sick-20160216-01321.

> recommendations associated with mitigating cybersecurity threats to device functionality and device users. (Line 72).

It is the last point in particular we want to emphasize. There are indeed a large number of stakeholders in the life cycle of cyber medical devices. The stakeholders are subject to different statutes and rules for privacy. For example, some stakeholders are covered entities subject to HIPAA privacy and security rules. Some are not. What that means is that PII produced by cyber medical devices will be regulated for privacy in the hands of some stakeholders and not regulated in other hands. In some cases, state privacy laws may apply to some stakeholders.

The data flow considerations here are significant: **as personally identifiable information from cyber medical devices passes from one stakeholder to another, there is a very real threat that the PII will lose (or gain) both state and federal legal privacy protections.**

Even worse, the expectations of an average use of a cyber medical device are that their personal data receives the same meaningful privacy protections wherever it goes. As we know too well today, health privacy laws at the federal and state level are complex, apply to some but not all processors of health PII, and are largely incomprehensible to the average American.[3]

The FDA cannot expect that users of devices will understand existing privacy law or be able to compensate for their weaknesses. The FDA needs to recognize the existing privacy legal environment and require that the relevant stakeholders fill gaps so that PII does not move from a regulated domain to one that has no rules at all. The FDA should provide that device manufacturers and other must step in and take actions that users cannot take on their own.

Additionally, as the FDA moves forward in its policymaking, privacy stakeholders need to be expressly included in its considerations and deliberations.

II. Need for more attention to privacy, and a suggestion about how to improve the NPRM in this area

While we welcome the FDA's attention to security for cyber medical devices, we do not think that there is enough emphasis on privacy in the draft guidance. In the context of medical devices, security serves several related purposes, with the protection of the privacy of personal information being one of those purposes. The FDA should address privacy in its guidance more deliberately than it does. We do not suggest, however, that the FDA is unaware of privacy. At line 310, the draft guidance states:

> "These [comprehensive cybersecurity risk management] programs should emphasize addressing vulnerabilities which may permit the **unauthorized access,**

[3] The World Privacy Forum addressed this issue in its publication, *A Patient's Guide to HIPAA*. It answers frequently asked questions about health privacy. Question 3 (What Federal Laws Are Relevant to Health Privacy?) takes almost a thousand words just to identify and briefly describe the federal health privacy laws. See FAQ 3, https://www.worldprivacyforum.org/2013/09/hipaaguidehome/. State health privacy laws add an additional level of complexity.

modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may impact patient safety. Manufacturers should respond in a timely fashion to address identified vulnerabilities. Critical components of such a program include:

> • Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
> • Understanding, assessing and detecting presence and impact of a vulnerability;
> • Establishing and communicating processes for vulnerability intake and handling;
> • Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
> • Adopting a coordinated vulnerability disclosure policy and practice; and
> • Deploying mitigations that address cybersecurity risk early and prior to exploitation."

We highlight here and welcome the existing words that address privacy matters. However, we do not think that the proposed program components are explicit enough with respect to privacy. We propose adding two additional items:

> • Controlling the processing (including access, use, maintenance, disclosure, modification, and other activities) of personally identifiable information and of information that could become personally identifiable throughout the entire life cycle of a device and the information.

> • Identifying gaps or conflicts in legal protections for personally identifiable information and providing contractual remedies to address existing shortcomings.

If the FDA secures the environment, but does not attend to the complexities of data protection legalities within the data flows, then we predict there will be many unexpected backlashes at a later point as data problems fester and eventually reach a point where they must be addressed. It is still possible for the FDA to help reduce unnecessary losses in this area by addressing the privacy complexities head-on and early in the cycle.

Similarly, the section of the draft guidance that begins at line 380 and addresses Medical Device Cybersecurity Risk Management does not contain sufficient attention to privacy risk management. It is too easy for someone not familiar with both the commercial and criminal marketplaces for health information to underestimate the consequences of the loss or misuse of PII. We refer you by way of example to a recent WPF report titled: *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future.* [4] The report robustly

[4] Dixon, Pam and Gellman Robert, *The Scoring of America*, World Privacy Forum, April 2, 2014. https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

documents the then little known use of consumer information for predictive scoring in a largely unregulated commercial marketplace. Too few consumers and policy makers understand that marketplace.

We suggest that this section of the report include specific guidance like this:

Assessment of privacy risks must consider the gaps in legal protections for privacy, the commercial and criminal marketplaces for personal information, and the consequences to data subjects from the uncontrolled use and disclosure of their personally identifiable information.

III. Need for more public interest participation

The draft guidance acknowledges (line 99) the role of Information Sharing Analysis Organizations (ISAOs). ISAQs are intended by Executive Order 13691 to serve as focal points for cybersecurity information sharing and collaboration within the private sector as well as between the private sector and government. The guidance states expressly that it seeks "to promote collaboration among the medical device and Health IT community to develop a shared understanding of the risks posed by cybersecurity vulnerabilities to medical devices and foster the development of a shared understanding of risk assessment to enable stakeholders to consistently and efficiently assess patient safety and public health risks associated with identified cybersecurity vulnerabilities and take timely, appropriate action to mitigate the risks." (line 127). We acknowledge without further comment the existing role of ISAQs.

We recognize that these efforts are intended to be inclusive and broadly based. However, we are concerned that public interest and patient voices are not likely to be heard in these collaborations. As evidence, we point to the FDA's Memorandum of Understanding with the National Health Information Sharing & Analysis Center. See http://www.nhisac.org/. We do not question the bona fides of this Center, but we observe that its Board of Directors consists of representatives of more than a dozen major health care institutions, and no public interest or patient group are represented on the Board. The minimum cost of membership is $3000 for a non-profit, a cost that is prohibitive for many if not most public interest organizations. Cost of attending meetings is another barrier for small non-profit public and patient interest organizations.

The FDA operates in a world where many companies in the health sector have revenues measured in the **billions** or **tens of billions** of dollars. These organizations have the resources to go to meetings and collaborate when promoted to do so by their regulators. This is not always the case for public interest or patient groups.

We recommend that the FDA say expressly that it expects that cybersecurity activities must involve public interest and patient groups that choose to participate. Companies that fund these efforts should be encouraged, if not required, to fund public interest and patient groups that have relevant expertise and are willing to participate.

We want to make it clear that the World Privacy Forum is not seeking funding for this purpose. We have in mind an organization like the Electronic Frontier Foundation that has relevant technical and policy expertise in cybersecurity. There are also many academics with

cybersecurity skills that might be useful public interest representatives if they had financial support for their activities.

We thank the FDA for the opportunity to comment on the draft guidance. We stand ready to help. We also urge the FDA to understand that privacy is not an onerous obstacle to forward progress. It can become a problem when it is segregated from security, and when crucial issues are ignored or sidestepped at the outset. In those conditions problems can grow into something unmanageable down the road. Health data breaches and medical identity theft are two such examples of this in the health sphere. Doing the right thing here, particularly regarding legal protections and data flows, is the ounce of prevention that is worth its weight in gold later on down the line.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum