MICHIGAN ENGINEERING
UNIVERSITY of MICHIGAN ■ COLLEGE of ENGINEERING

COMPUTER SCIENCE AND ENGINEERING
BOB AND BETTY BEYSTER BUILDING
2260 HAYWARD STREET
ANN ARBOR, MICHIGAN 48109-2121
734 764-1688
cse.umich.edu

April 21, 2016

Dr. Suzanne Schwartz
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Ave., Bldg. 66, Rm. 5418
Silver Spring, MD 20993-0002

Dear Dr. Suzanne Schwartz,

Thank you for the opportunity to respond to Docket No. FDA-2015-D-5105 for "Postmarket Management of Cybersecurity in Medical Devices." I would like to commend the FDA leadership for waking up from its cyberslumber in the 2000s and moving beyond the former "let's all just get along on cybersecurity" policies to more meaningful cybersecurity guidance with specific responsibilities assigned to specific stakeholders. I appreciate that FDA has invested four years to thoughtfully respond to the NIST ISPAB letter's primary recommendation to improve postmarket surveillance of cybersecurity threats [20]. The proposed guidance will help HDOs begin to more meaningfully cope with cybersecurity threats against medical devices and the delivery of healthcare. Stakeholders need to communicate cybersecurity vulnerabilities and incidents more effectively, and monitor for shifting threats. Medical device manufacturers should create frictionless workflows to receive outside input on potential vulnerabilities.

Credentials and experience. I represent the academic medical device security community. I am Associate Professor of Computer Science & Engineering at the University of Michigan where I conduct research on computer security and healthcare as part of the National Science Foundation's Trustworthy Health and Wellness (THAW.org) Frontiers project and HHS ONC's Strategic Healthcare IT Advanced Research Projects on Security (SHARPS.org). Michigan teaches computer security to 500+ students each year. My educational qualifications include a Ph.D., master's degree, and bachelor's degree from MIT. I began working in hospital IT in the early 1990s. My PhD dissertation solved problems of high performance encryption and authentication of data at rest and in transit. I have given nearly 100 invited talks on medical device security to industry, government, and academia—including Senate and House hearings, the Institute of Medicine, and National Academy of Engineering events. I direct the Archimedes Center for Medical Device Security at the University of Michigan. I co-founded the healthcare cybersecurity company Virta Labs. My participation in the 2008 IEEE paper analyzing the security of a defibrillator led to a wake-up call for medical device manufacturing [15]. I co-chaired the AAMI Working Group on Medical Device Security, which led to the the AAMI TIR57 document that advises medical device manufacturers on how to incorporate security engineering into medical device product development. I co-authored the NIST Information Security and Privacy Advisory Board recommendations [20] to HHS on how the federal government must adapt to risks of medical device security. Beginning with my 2006 security seminar at FDA CDRH, my medical device security efforts were recognized with a Fed100 Award, Sloan Research Fellowship, NSF CAREER Award, MIT TR35 Innovator of the Year award, and best paper awards on medical device security by organiziations such as IEEE and ACM [3, 16, 13, 9, 10, 5, 19, 18, 8, 6, 14, 2, 12, 21, 11]. My previous affiliations include MIT CSAIL, FDA, the Beth Israel Deaconess Medical Center of Harvard Medical School, Microsoft Research, HP Labs, UMass Amherst, Cisco Systems, Bellcore, and Holland Community Hospital.

Comments on the draft postmarket cybersecurity guidance:

1. Lines 19–22: Any effective postmarket approach must be comprehensive and agnostic of modality of how risks enter a clinical setting. The draft document refers to "network connected" and "connected" several times, but the document ought instead refer to **"exposure to cybersecurity risks."** The subtle difference is key because the former terms treat *symptoms* whereas the more technically correct phrase I suggest focuses on *outcomes*. Just as we would not write a guidance document on how to avoid catching the flu spread by sneezing while excluding flu spread by cough, the FDA guidance document on postmarket cybersecurity should not focus on modality of an infection vector, but rather outcomes. The number of infection vectors is unknown and constantly shifting, so it would be unwise to write a document that focuses so much on a single pathway: networks. Things ignored by such definitional language include: USB drives, social engineering by telephone, CDROMs, and even tape drives and floppy drives still in use by hospitals.

   The terms "networked devices" and "connected" are red herrings. A network is not necessary for a cybersecurity exploit; malware gets in just fine by unhygienic USB drives carried by unsuspecting personnel or medical device sales engineers. Hackers continue to use social engineering by telephone to trick personnel into giving out unauthorized remote access. The final postmarket guidance will need to more deliberately draw attention to **outcomes** of compromise and risks of vulnerabilities rather than the constantly evolving **modality** of delivery of exploits. Should the guidance document list networked and connected devices as examples of infection vectors? Yes. Should it mention only networked and connected devices? No. Focus on outcomes, not modalities. Moreover, network-based postmarket surveillance alone would not catch risks such as intentional electromagnetic interference that can compromise externally worn sensors [7]. Individual clinicians and vendors often work for multiple HDOs, and carry USB drives across protection boundaries. Thus, hospital A can infect hospital B without a network connection.

   I recommend FDA use language such as "exposed to cybersecurity risk" instead of "networked" or "connected" when discussing overall objectives because cybersecurity threats are constantly evolving.

2. I recommend caution and skepticism when enrolling and periodically reviewing the effectiveness of ISAOs. ISAOs are important, but sharing of data is not useful if the data are not high quality. For instance, one hospital uses a vulnerability scanner to automatically generate trouble tickets. One trouble ticket resulted from a warning of an SSH server with an outdated cipher suite vulnerable to a known attack. To mitigate the warning, the hospital turned off

the SSH server and turned on an insecure telnet server that no longer produces a security warning of an outdated cipher suite. And yet telnet servers are trivially compromised. Sharing of poor quality information could actually cause harm just as anti-virus products have been known to occasionally cause unscheduled downtime of clinical systems[1].

3. The postmarket guidance does not presently catch cybersecurity problems of the distribution of postmarket software updates. For instance, I documented in 2012 how a medical device manufacturer was a victim of an SQL injection attack that compromised their website such that biomedical engineers downloading ventilator firmware updates also received a "bonus" piece of malware. This malware, known as a drive-by download, likely compromised the PCs of any biomedical engineer who downloaded the firmware update[2]. Early warnings on authenticity of software updates for medical devices appeared at USENIX HotSec in 2006 [1].

4. The postmarket guidance does not presently catch cybersecurity problems of vendors who accidentally spread malware in HDOs while repairing medical devices. Lynette Sherrill of the VA Field Security office reported that a 3rd party vendor infected VA systems with malware by accident while performing software updates. A former engineer from vendor of a pharmaceutical compounder explained that when the drug mixing machine running Windows XP was compromised by malware, the repair technicians accidentally spread the malware to the other compounders under repair.

5. Based on the two previous points, **the guidance should include language that acknowledges the risks of unauthentic software updates**, not limited to downloaded updates (since physical installation media can carry malware) and not limited to the devices being updated. Installation of updates should be conducted in a hygienic computing environment, and compensating controls such as anti-virus should not be turned off while the updates are in progress. Suggested language: **"Manufacturers must enable HDOs to cryptographically authenticate software updates using a NIST recommended use case."**

6. The first use of the MedWatch 3500 form for FDA to take notice of a cybersecurity vulnerability took over a year [16] to be processed into the FDA MAUDE database of adverse events. I am pleased to see that FDA recognizes that a mechanism other than MAUDE is needed for rapid sharing of cybersecurity threats, vulnerabilities, and incidents. However, adverse events are still adverse events. **The guidance should include language that emphasizes the continued importance of adverse-event reporting**, and emphasizes that adverse events related to security, including malware infestations, are still adverse events. Furthermore, the guidance should include language that encourages HDOs to report security-related events that occur during software updating: **"HDOs and manufacturers should continue to use MAUDE to report security-related adverse events that result in a malfunction, injury, or harm."**

7. Network monitoring is only one of many ways to carry out postmarket surveillance of cybersecurity threats. For instance, Clark et al. demonstrated how to use special power outlets to detect malware that can hold a medical device for ransom [4].

8. Today, there is little reproducible, refutable science on postmarket surveillance of cybersecurity risks in HDOs. In my own research, we found gaping holes in postmarket cybersecurity

[1] http://blog.secure-medicine.org/2014/04/when-anti-virus-updates-goes-awry.html

[2] http://blog.secure-medicine.org/2012/06/click-here-to-download-your-avea.html

data [17] that lulled the industry and government into a false sense of security for years.

9. FDA should separate expectations of patch time from incident discovery time. For instance, simply discovering malware within a few minutes of infection instead of 200 days would immediately reduce risks to HDO infrastructure by reducing exposure. A machine ought to be quarantined away from other vulnerable machines if a patch is not readily available. Unlike traditional safety goals where statistics can help predict the likelihood of hazards matriculating into harm, statistics of computer security problems are notoriously misleading as adversaries are sentient and react to defenses. Adversaries only get smarter and more effective over time so long as cybersecurity problems remain economically profitable, as evidenced by the recent outbreak of ransomware in hospitals.

10. I recommend that FDA continue to follow the advice of NIST. Drawing on NIST cybersecurity guidance for critical infrastructure, a few of the key postmarket activities that HDOs and medical device manufacturers ought to follow to manage cybersecurity risks: (1) enumerate cybersecurity risks because deploying technology without understanding risk is counterproductive, (2) deploy cybersecurity controls that match the specific risks, (3) continuously measure the effectiveness of the security controls because threats, vulnerabilities, and misconfigurations can bypass a previously effective control within seconds.

11. Economic impact. I believe that costs will decrease for HDOs in the long run once effective postmarket cybersecurity is implemented because the surveillance will lead to more trustworthy medical devices that have improved safety, efficacy, and security. HDO staff presently assigned to uncoordinated guessing of cybersecurity problems will be able to return to their core mission of the delivery of healthcare.

Respectfully submitted,

Kevin Fu
Associate Professor
Computer Science & Engineering
University of Michigan
fugistics@umich.edu

References

[1] A. Bellissimo, J. Burgess, and K. Fu. Secure software updates: disappointments and new challenges. In *Proceedings of USENIX Hot Topics in Security (HotSec)*, July 2006. https://spqr.eecs.umich.edu/papers/secureupdates-hotsec06.pdf.

[2] W. P. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In *Proceedings of the 49th Design Automation Conference*, DAC '12, June 2012. Invited paper https://spqr.eecs.umich.edu/papers/49SS2-3_burleson.pdf.

[3] S. S. Clark and K. Fu. Recent results in computer security for medical devices. In *International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth), Special Session on Advances in Wireless Implanted Devices*, Oct. 2011. https://spqr.eecs.umich.edu/papers/clark-mobihealth11.pdf.

[4] S. S. Clark, B. Ransford, A. Rahmati, S. Guineau, J. Sorber, W. Xu, and K. Fu. WattsUpDoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices. In *USENIX Workshop on Health Information Technologies*, Aug. 2013. https://spqr.eecs.umich.edu/papers/clark-healthtech13.pdf.

[5] B. Defend, M. Salajegheh, K. Fu, and S. Inoue. Protecting global medical telemetry infrastructure. Technical report, Institute of Information Infrastructure Protection (I3P), Jan. 2008. https://web.eecs.umich.edu/~kevinfu/papers/whitepaper-protecting_global_medical.pdf.

[6] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *Proceedings of USENIX Workshop on Hot Topics in Security (HotSec)*, July 2008. https://spqr.eecs.umich.edu/papers/watchdog-hotsec08.pdf.

[7] D. Foo Kune, J. Backes, S. S. Clark, D. B. Kramer, M. R. Reynolds, K. Fu, Y. Kim, and W. Xu. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *Proceedings of the 34th Annual IEEE Symposium on Security and Privacy*, May 2013. https://spqr.eecs.umich.edu/papers/fookune-emi-oakland13.pdf.

[8] K. Fu. Inside risks, reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care. *Communications of the ACM*, 52(6):25–27, June 2009. http://www.csl.sri.com/users/neumann/insiderisks08.html#218.

[9] K. Fu. Software issues for the medical device approval process, Apr. 2011. Statement to the Special Committee on Aging, United States Senate, Hearing on a delicate balance: FDA and the reform of the medical device approval process, Wednesday, April 13, 2011 https://spqr.eecs.umich.edu/papers/fu-senate-comm-aging-med-dev-sw-apr-2011.pdf.

[10] K. Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, Washington, DC, July 2011. IOM (Institute of Medicine), National Academies Press https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf.

[11] K. Fu. On the technical debt of medical device security. Technical report, National Academy of Engineering FOE, Sept. 2015. http://www.naefrontiers.org/File.aspx?id=50750. A version appeared in the National Academy of Engineering's *The Bridge*.

[12] K. Fu and J. Blum. Inside risks: Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 56(10):21–23, Oct. 2013. http://www.csl.sri.com/users/neumann/cacm231.pdf.

[13] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implanted medical devices. In *Proceedings of ACM SIGCOMM*, Aug. 2011. https://spqr.eecs.umich.edu/papers/gollakota-SIGCOMM11-IMD.pdf.

[14] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, 7(1):30–39, Jan. 2008. `https://spqr.eecs.umich.edu/papers/b1kohFINAL2.pdf`.

[15] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, pages 129–142, May 2008. `https://www.secure-medicine.org/publications/icd-study.pdf`.

[16] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song. Take two software updates and see me in the morning: The case for software security evaluations of medical devices. In *Proceedings of 2nd USENIX Workshop on Health Security and Privacy (HealthSec)*, Aug. 2011. `https://spqr.eecs.umich.edu/papers/hanna-aed-healthsec11.pdf`.

[17] D. B. Kramer, M. Baker, B. Ransford, A. Molina-Markham, Q. Stewart, K. Fu, and M. R. Reynolds. Security and privacy qualities of medical devices: An analysis of FDA postmarket surveillance. *PLoS ONE*, 7(7):e40200, July 2012. `http://journals.plos.org/plosone/article/asset?id=10.1371/journal.pone.0040200.PDF`.

[18] S. Lee, K. Fu, T. Kohno, B. Ransford, and W. H. Maisel. Clinically significant magnetic interference of implanted cardiac devices by portable headphones. *Heart Rhythm Journal*, 6(10):1432–1436, Oct. 2009. `http://bit.ly/1NEk3dR` or `http://download.journals.elsevierhealth.com/pdfs/journals/1547-5271/PIIS1547527109007401.pdf`.

[19] A. D. Molina, M. Salajegheh, and K. Fu. HICCUPS: Health information collaborative collection using privacy and security. In *Proceedings of the Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pages 21–30. ACM Press, Nov. 2009.

[20] NIST ISPAB federal advisory commmittee recommendations on improving medical device cybersecurity, 2012. Sent to OMB Director, HHS Secretary, NSC, DHS, NIST, March 30, 2012 `http://1.usa.gov/1qlnh0X` or `http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_med_device.pdf`.

[21] M. Salajegheh, A. Molina, and K. Fu. Privacy of home telemedicine: Encryption is not enough. *Journal of Medical Devices*, 3(2), Apr. 2009. Design of Medical Devices Conference Abstracts `https://spqr.eecs.umich.edu/papers/salajegheh-DMD09-abstract.pdf`.