BMJ Open

Cybersecurity Features of Digital Medical Devices: An Analysis of FDA Product Summaries

Journal:	*BMJ Open*
Manuscript ID	bmjopen-2018-025374
Article Type:	Research
Date Submitted by the Author:	11-Jul-2018
Complete List of Authors:	Stern, Ariel; Harvard Business School Technology and Operations Management; Harvard-MIT Center for Regulatory Science Gordon, William; Brigham and Women's Hospital Department of Medicine; Harvard Medical School Landman, Adam; Brigham and Women's Hospital Department of Medicine Kramer, Daniel; Beth Israel Deaconess Medical Center, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology; Harvard Medical School
Keywords:	Medical Devices, Software, Cybersecurity, FDA, Regulatory Policy

CYBERSECURITY FEATURES OF DIGITAL MEDICAL DEVICES:

AN ANALYSIS OF FDA PRODUCT SUMMARIES

Ariel D Stern, Assistant Professor Harvard Business School, the Harvard-MIT Center for Regulatory Science, Morgan Hall 433, Soldiers Field Rd, Boston, MA 02163, astern@hbs.edu

William J Gordon, Instructor of Medicine, Division of General Internal Medicine, Brigham and Women's Hospital, Harvard Medical School, 1620 Tremont Street, Boston, MA 02120, wgordon@partners.org

Adam B Landman, Chief Information Officer, Brigham and Women's Hospital, Harvard Medical School, 75 Francis St, Boston, MA 02115, alandman@bwh.harvard.edu

Daniel B Kramer, Assistant Professor of Medicine, Harvard Medical School, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology, Beth Israel Deaconess Medical Center, Baker 4, West, 330 Brookline Ave, Boston, MA 02115, dkramer@bidmc.harvard.edu

Correspondence to: Ariel D Stern

Keywords: Medical Devices, Software, Cybersecurity, FDA

Word Count: 1,850

Structured Abstract

Objectives: In order to more clearly define the landscape of digital medical devices subject to U.S. Food and Drug Administration (FDA) oversight, this analysis leverages publicly-available regulatory documents to characterize the prevalence and trends of software and cybersecurity features in regulated medical devices.

Design: We analyzed data from publicly available FDA product summaries to understand the frequency and recent time trends of inclusion of software and cybersecurity content in publicly available product information.

Setting: The full set of regulated medical devices, approved over the years 2002-2016 included in the FDA's 510(k) and premarket approval databases.

Primary and secondary outcome measures: The primary outcome was the share of devices containing software that included cybersecurity content in their product summaries. Secondary outcomes were differences in these shares a) over time and b) across regulatory areas.

Results: Among regulated devices, 13.79% were identified as including software. Among these products, only 2.13% had product summaries that included cybersecurity content over the period studied. The overall share of devices including cybersecurity content was higher in recent years, growing from an average of 1.4% in the first decade of our sample to 5.5% in 2015 and 2016, the most recent years included. The share of devices including cybersecurity content also varied across regulatory areas from a low of 0% to a high of 22.2%.

Conclusions: To ensure the safest possible health care delivery environment for patients and hospitals, regulators and manufacturers should work together to make the software and cybersecurity content of new medical devices more easily accessible.

Article Summary

Strengths and limitations of this study

- Cybersecurity issues related to medical devices have been documented in individual cases, but the inclusion of cybersecurity content has never been considered systematically; we provide the first such analysis.
- The study also provides a new application of the use of the Medical Text Indexer – a document classification algorithm from the U.S. National Library of Medicine – for understanding the content of medical product descriptions.
- The study's primary limitation is that because the inclusion of cybersecurity content is not mandatory in FDA product summary documents, some devices may include cybersecurity features that cannot be accounted for by this analysis.

Introduction

The United States (US) National Research Council (NRC) defines cybersecurity as "the technologies, processes, and policies that help to prevent and/or reduce the negative impact of events…that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor."[1] In the US, the Cybersecurity Information Sharing Act of 2015 included health care provisions (Sec. 405), requiring that the Department of Health and Human Services to report to Congress regarding the preparedness of the health care industry in responding to cybersecurity threats, acknowledging these risks and laying out reporting requirements.[2] In health care delivery and health care policy, cybersecurity comes up most readily in the context of health information technology. Such technology may include stand-alone software, such as electronic health record systems, or combinations of hardware and software, such as those seen in modern pacemakers, blood glucose monitors, and computed tomography scanners. In the latter category, many digital products pose sufficient risk to patients as to require regulatory approval for use. In the US, products containing both software and hardware are regulated by the US Food and Drug Administration (FDA). Importantly, digital medical devices – those that contain software and/or digital networking capabilities – are quickly becoming embedded in all facets of medical care. However, the prevalence of software and the inclusion of cybersecurity features among already-marketed regulated medical devices have not been previously investigated.

At the same time, there have been several recent examples of software-related medical device vulnerabilities,[3,4] including potential use of a pacemaker remote monitoring system to issue malicious programming commands.[5] These devices may also place health care facilities at risk:[6] A recent report from a cybersecurity firm highlighted the fact that 90% of hospitals had

been targeted by cybercriminals in the past two years and that 17% of these documented attacks had been facilitated by Internet-connected medical devices.[7] The May 2017 WannaCry ransomware attack was the largest cyberattack to affect the United Kingdom's National Health Service, impacting 34% of trusts and disrupting some medical devices, including a subset of MRI scanners and devices to test blood and tissue samples.[8,9]

In recognition of these risks, the FDA has issued both pre and post-market regulatory guidance[10,11] on medical device cybersecurity while actively engaging industry and outside experts in addressing post-market cybersecurity concerns. In order to more clearly define the landscape of digital medical devices subject to FDA oversight, this analysis leverages publicly-available FDA documents to characterize the prevalence and trends of software and cybersecurity features in regulated medical devices.

Methods

Data Sources

We analyzed data from publicly available FDA product summaries, identified from searchable documents published by the FDA at the time of each new device's clearance or approval for marketing.[14,15] Such summaries have supported previous analyses,[16,17] and, as outlined by FDA guidance, these summaries contain information such as indications for use, a detailed device description (including device design, material use, and physical properties), contradictions/warnings/precautions, and clinical evidence supporting the regulatory assessment of safety and effectiveness.[18,19] Along with the FDA-approved product label (with which a summary will share many pieces of important information), summary documents represent key

pieces of publicly available information about medical devices that have been granted marketing approval.

We used the FDA's 510(k) and premarket approval (PMA) databases to identify all new device clearances and approvals from 2002-2016, respectively[14,15] (see **Supplementary Material**). In brief, under the FDA's risk-based framework for premarket evaluation,[20] high-risk devices are evaluated under the PMA pathway, which includes demonstration of clinically-relevant safety and effectiveness. By contrast, medium-risk devices are generally assessed via the "510k" pathway, which evaluates whether new safety or effectiveness concerns are raised by the device at issue compared to a "substantially equivalent" device already on the market.[21] We identified the eight largest medical device categories by advisory committee of assignment, which accounted for over 75%[14,15] of all regulated devices that came to market over this period of time (see **Exhibit 1**). Modifications to already-marketed devices approved via the PMA supplement pathway[22] were excluded.

We used an automated script to batch download all associated product summaries and applied *ABBYY FineReader* optical character recognition software (ABBYY, Milpitas, CA) to convert these Portable Document Format (PDF) files into machine-readable text files.

Analysis Sample

We used the US National Institute of Health's National Library of Medicine (NLM) *Medical Text Indexer*[23] (MTI) to identify digital devices as those referencing and/or describing software in their product summaries. The MTI uses natural language processing algorithms that take free text as input and provide medical subject indexing recommendations, based on the MeSH® vocabulary[24] established by the NLM, as output. From a regulatory perspective,

products containing software must mention this in their summaries (see above). Indeed, many device summaries contain a short section of the document that is dedicated to describing the product's software (for example, as seen for the Medtronic MiniMed 670G Automated Insulin Delivery System).[25] We used the sample of summaries that were flagged by the MTI as including the medical subject of "software" as our analysis sample of digital devices ("software sample"). In sensitivity analysis, an alternative, keyword-based definition was considered and did not impact findings (**Supplementary Material**). For each product in the software sample, we recorded each device's FDA decision date (i.e. the year in which the product came to market), its regulatory approval pathway (510(k) or PMA), and the reviewing advisory committee.

Characterization of Cybersecurity Features

The "cybersecurity features" of digital medical devices can take on a number of forms, each of which can address the risks of actions by malevolent parties. Such cybersecurity features may include characterizations or descriptions of a digital product's defensive abilities (e.g. data encryption), an ability to respond to a security breach should it be attempted (e.g. antivirus software), or the ability to detect a breach that has already occurred (e.g. penetration testing).

We searched each of the summaries in the software sample for a pre-specified list of keywords related to cybersecurity content (**Supplementary Material**) and documented use of these keywords (yes/no) in each product summary. These keywords and phrases were selected *a priori* from terminology glossaries from the US National Initiative for Cybersecurity Careers and Studies (NICCS), the FDA's guidance on cybersecurity for medical devices, the US National Institute of Standards and Technology (NIST 4009 / NISTIR 7298) Glossary,[26] and the Manufacturer Disclosure Statement for Medical Device Security (MDS2), a multi-stakeholder

devised form designed to give manufacturers a mechanism of disclosing security-related product information to healthcare providers.[27]

Data Analysis

For each year, we identified the software sample and calculated the number and percentage (share) of devices that included cybersecurity content by advisory committee and overall. We compared the percentage of devices with cybersecurity content, as identified by keywords. Using chi-squared tests, we looked at differences between the two major regulatory approval pathways and in earlier versus later years.

In order to validate our automated search protocol, we manually reviewed 50 summaries from the software sample that were identified as containing cybersecurity information, and 50 that were identified as having no such content to confirm text scraping methods. Discrepancies were reviewed by group assent. We further validated our method of identifying devices containing software by electronically scanning all product summaries for the keyword "software" and using these results to assess the sensitivity and specificity of the MTI-defined software sample. (**Supplementary Material**).

All analyses were conducted in STATA version 14.2 (StataCorp LLC, College Station, TX).

Results

A total of 36,430 new devices were identified (**Exhibit 2**) and of those, 35,794 (98.3%) had product summaries that could be converted to machine-readable text. From this sample, 4,936 new devices (13.79%) were identified by the MTI as including software (9.70% of PMA

devices and 13.82% of 510(k) devices. Within the software sample, we found that only 2.13% of devices had product summaries that included cybersecurity content (3.45% of PMA devices and 2.12% of 510(k) devices, however, differences were not statistically significant [p=0.62]). Manual review confirmed that 100% of summaries included the keyword(s) found by our automated program. Relative to our keyword-based validation exercise, the MTI has a sensitivity of 100% and a specificity of 94.8%, making it a more conservative measure.

Exhibit 3a presents the share of devices with software over time, while **Exhibit 3b** presents the share of devices in the software sample that included cybersecurity content in their product summaries over the same period. The overall share of devices including cybersecurity content was higher in recent years, growing from an average of 1.4% in the first decade of our sample to 5.5% in 2015 and 2016, the most recent years included (p = 0.0181). The share of devices including cybersecurity content also varied across regulatory areas from a low of 0% across all years in gastroenterology/urology devices, orthopedic devices, and general/plastic surgery devices, to a high of 22.2% among general hospital devices in 2016 (**Exhibit 1**).

Comment

This study leverages a novel methodology to create an analyzable dataset from public documents describing newly-marketed medical devices. We found that software is an increasingly common component of newly approved or cleared devices, while cybersecurity content in the devices' publicly available summaries remains rare.

As more and more aspects of healthcare are digitized, the cybersecurity of our healthcare infrastructure—including medical devices—will be increasingly essential to delivering safe and effective care. Recent events such as the emergence of pacemaker vulnerabilities have

highlighted both the public health implications of information security[28] and importance of device security.[6] Additionally, the recent security flaws discovered in widely-used computer processors, highlight the fact that new threats continue to unfold[29] with the opportunity for significant clinical impact. Indeed, the NRC has written that "from the standpoint of an individual system or network operator, the only thing worse than being penetrated is being penetrated and not knowing about it."[1] Our work is an important first step in a public, transparent understanding of the cybersecurity features included in the software embedded in moderate- and high-risk medical devices.

Importantly, product summaries may not include all relevant details of device design with respect to cybersecurity. While this information may exist in other places, such as proprietary applications or the full, confidential FDA dossier, device summaries represent some of the primary documents available for public review, and therefore play an important role in educating stakeholders, such as clinicians, purchasing managers, patients, and administrators of health care systems, about the strength of safety and effectiveness evidence when a new product comes to market.

These findings help define the current landscape of medical device software and cybersecurity features, and suggest an opportunity to better inform healthcare professionals, those engaging in device procurement on behalf of hospitals and health care systems, and patients, on the cybersecurity protections embedded in medical devices. In an increasingly digitized health care ecosystem, manufacturers will face increasing demands for product safety in the form of cybersecurity protections. Moreover, stakeholders will increasingly seek out information about the safety features of new products. The FDA and manufacturers should work together to make the software and cybersecurity content of new products more easily accessible,

and should continue to work together to determine which cybersecurity content should be disclosed and required for regulatory clearance and approval of new products moving forward.

Author Contributions: ADS designed the study in consultation with WJG, ABL, and DBK. ADS collected the data from public sources and performed the primary analysis. All authors had full access to the data and analysis programs for this study and take responsibility for the integrity of the data and the accuracy of the analysis. All authors wrote the manuscript.

Data Sharing Statement: Statistical code and the full dataset are available at https://github.com/arieldora/SternCybersecurityContent

Conflicts of Interest: Dr. Kramer is supported by the Greenwall Faculty Scholars Program in Bioethics, is a consultant to Circulatory Systems Advisory Panel of the Food and Drug Administration, and has provided consulting to the Baim Institute for Clinical Research for clinical trials of medical devices (unrelated to the study topic). There are no other financial or commercial financial conflicts of interest related to the study topic to report.

Funding: The Harvard Business School Division of Research and Faculty Development supported the data collection for this study.

References

1. National Research Council. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues [Internet]. The National Academies Press; 2014 [cited 2018 Feb 5]. Available from: https://doi.org/10.17226/18749

2. Burr R. S.754 - 114th Congress (2015-2016): To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. [Internet]. 2015 [cited 2018 Apr 16]. Available from: https://www.congress.gov/bill/114th-congress/senate-bill/754

3. Blau M. Hospitals brace for security risks that could come with using wearables for patient care [Internet]. STAT. 2017 [cited 2018 Feb 5]. Available from: https://www.statnews.com/2017/08/04/hospitals-security-risks-wearables/

4. Kuchler H. Medical device makers wake up to cyber security threat. Financial Times [Internet]. 2017 Aug 1; Available from: https://www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691

5. Kramer DB, Fu K. Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. JAMA. 2017 Dec 5;318(21):2077–8.

6. Fox-Brewster T. Medical Devices Hit By Ransomware For The First Time In US Hospitals [Internet]. Forbes. 2017 [cited 2018 Feb 5]. Available from: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4a76dbe8425c

7. IoT guardian for the healthcare industry [Internet]. ZingBox; 2016. Available from: http://www.zingbox.com/wp-content/uploads/2017/02/ZingBox_WP_IoT-Guardian-for-the-Healthcare-Industry.pdf

8. Hughes O. WannaCry impact on NHS considerably larger than previously suggested [Internet]. Digital Health. 2017 [cited 2018 Feb 5]. Available from: https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/

9. Department of Health. Investigation: WannaCry cyber attack and the NHS [Internet]. 2017 Oxtober. Report No.: HC 414. Available from: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

10. Food and Drug Administration. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff. Available from: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

11. Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff. Available from:

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

12. Food and Drug Administration. Cybersecurity. 2018 Feb 2; Available from: https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

13. Food and Drug Administration. Digital Health Software Precertification (Pre-Cert) Program. 2017 Nov 15; Available from: https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/Default.htm

14. 510(k) Premarket Notification. 2017; Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPMN/pmn.cfm

15. Premarket Approval (PMA). 2018; Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPMA/pma.cfm

16. Zheng SY, Dhruva SS, Redberg RF. Characteristics of Clinical Studies Used for US Food and Drug Administration Approval of High-Risk Medical Device Supplements. JAMA. 2017 Aug 15;3187:619–25.

17. Dhruva SS, Bero LA, Redberg RF. Strength of study evidence examined by the FDA in premarket approval of cardiovascular devices. JAMA. 2009 Dec 23;302(24):2679–85.

18. Content of a 510(k). 2017 Oct 31; Available from: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/ucm142651.htm#link_7

19. PMA Application Contents. 2018 Feb 2; Available from: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm050289.htm#ssed

20. Kramer DB, Kesselheim AS. User Fees and Beyond — The FDA Safety and Innovation Act of 2012. N Engl J Med. 2012 Oct 4;367(14):1277–9.

21. Kramer DB, Xu S, Kesselheim AS. Regulation of Medical Devices in the United States and European Union. N Engl J Med. 2012 Mar 1;366(9):848–55.

22. Rome BN, Kramer DB, Kesselheim AS. FDA approval of cardiac implantable electronic devices via original and supplement premarket approval pathways, 1979-2012. JAMA. 2014 Jan 22;311(4):385–91.

23. NLM Medical Text Indexer (MTI). 2018; Available from: https://ii.nlm.nih.gov/MTI

24. MeSH [Internet]. [cited 2018 Feb 5]. Available from: https://www.ncbi.nlm.nih.gov/mesh

25. Summary of Safety and Effectiveness Data (SSED) [Internet]. Available from: https://www.accessdata.fda.gov/cdrh_docs/pdf10/P100034b.pdf

26. Kissel R. Glossary of Key Information Security Terms [Internet]. 2013 p. 1–218. Available from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

27. Manufacturer Disclosure Statement for Medical Device Security (MDS2). 2017; Available from: http://www.himss.org/resourcelibrary/MDS2

28. Gordon WJ, Fairhall A, Landman A. Threats to Information Security — Public Health Implications. N Engl J Med. 2017 Aug 24;377(8):707–9.

29. Metz C, Perlroth N. Researchers Discover Two Major Flaws in the World's Computers. The New York Times [Internet]. 2018 Jan 3 [cited 2018 Apr 17]; Available from: https://www.nytimes.com/2018/01/03/business/computer-flaws.html

Table 1: Number of devices with machine-readable summaries by FDA/CDRH Advisory Committee and year, share with software and share of software sample with cybersecurity content by Advisory Committee

	FDA/CDRH Advisory Committee								
Year	Clinical Chemistry (CH)	Cardiovascular (CV)	Dental (DE)	Gastroenterology, Urology (GU)	General Hospital (HO)	Orthopedic (OR)	Radiology (RA)	General, Plastic Surgery (SU)	Totals
2002	216	436	318	215	328	403	290	367	2573
2003	192	441	295	233	329	389	329	357	2565
2004	204	395	284	195	270	464	345	319	2476
2005	155	389	245	166	262	480	310	331	2338
2006	197	412	293	142	244	442	338	362	2430
2007	153	358	283	160	257	444	271	319	2245
2008	149	387	279	139	207	477	325	370	2333
2009	130	442	268	155	254	432	290	316	2287
2010	121	390	245	157	280	428	235	312	2168
2011	163	428	258	141	241	542	347	285	2405
2012	155	426	240	166	282	551	344	302	2466
2013	185	428	235	153	202	554	346	301	2404
2014	130	400	225	199	245	583	385	342	2509
2015	108	392	244	179	174	575	340	322	2334
2016	95	368	230	171	204	464	375	354	2261
Totals	2353	6092	3942	2571	3779	7228	4870	4959	35794
Share with software ("software sample")	9.14%	18.99%	4.59%	8.01%	4.97%	1.36%	52.28%	6.96%	13.79%
Share of software sample with cybersecurity content	7.91%	2.51%	1.66%	0.00%	2.13%	0.00%	2.04%	0.00%	2.13%

CYBERSECURITY FEATURES OF DIGITAL MEDICAL DEVICES:

AN ANALYSIS OF FDA PRODUCT SUMMARIES

Accompanying figures

Figure 1. Assembly of analysis sample and results

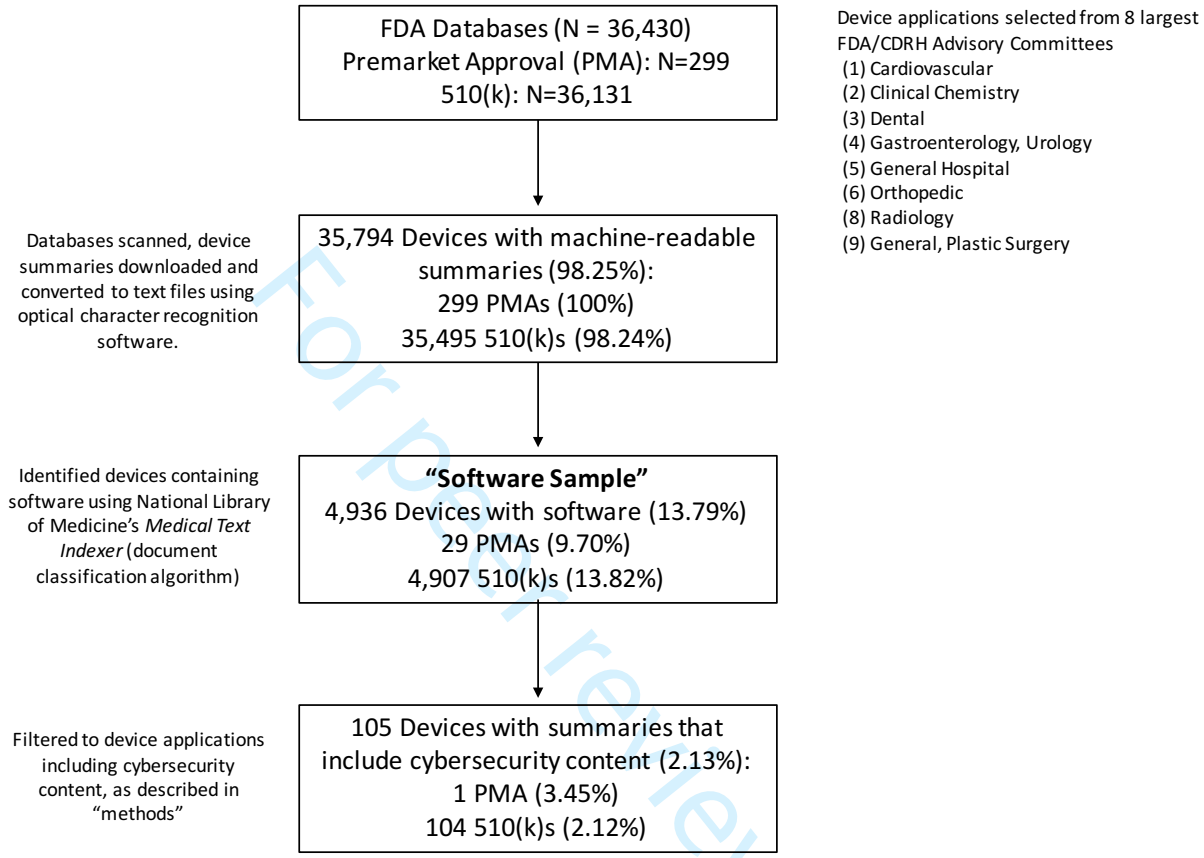


Figure 2

Figure 2a

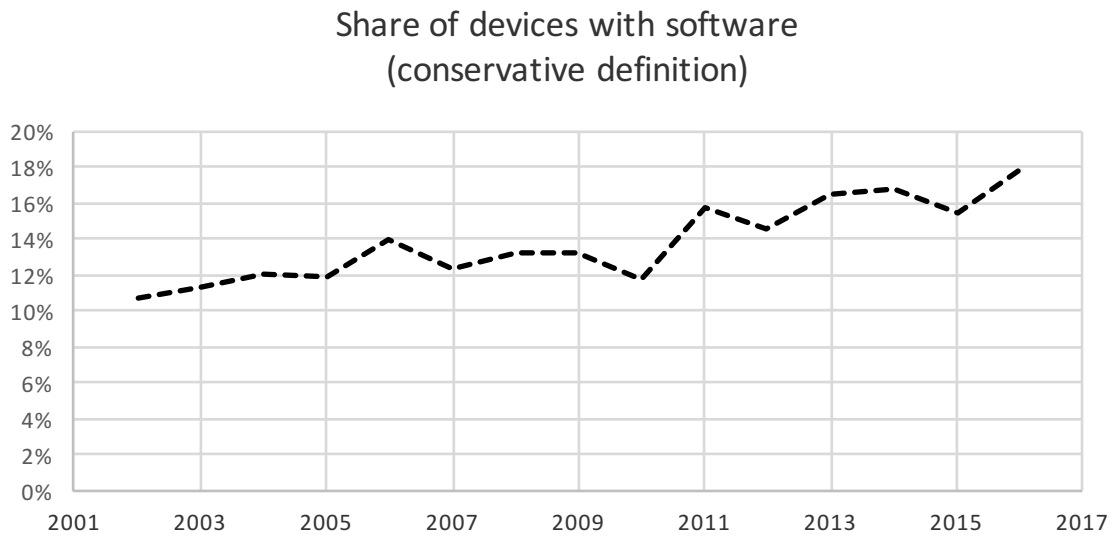
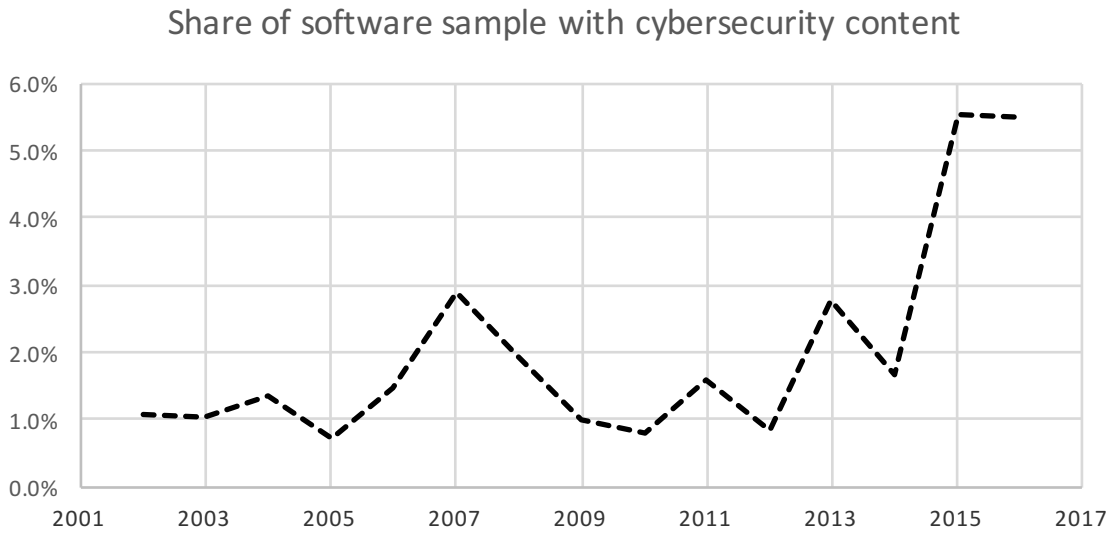


Figure 2b



Supplementary Material

I. Processing Using the Medical Text Indexer (MTI)

We sent each of our optical character recognition-processed text files to the MTI and recorded which summaries were classified as being related to software In the MeSH® Tree (ontology). We flagged all products whose summaries were assigned to the "software" MeSH® term, number L01.224.900.

II. Sensitivity Analysis

In sensitivity analyses we considered an alternate method of identifying devices containing software. For this exercise, we electronically scanned each product summary for the keyword "software" and recorded whether the word "software" appeared anywhere within a device's product summary (i.e. at least once in the document).

We expected that the MTI-driven method of identifying the "software sample" would have a high sensitivity but a lower specificity relative to the keyword-based method for the following reason: in order for a text document to be flagged by the MTI's algorithm as being related to the subject of "software" the text document would need describe relevant software content in some detail – i.e. often beyond simply utilizing the keyword "software" at least once.

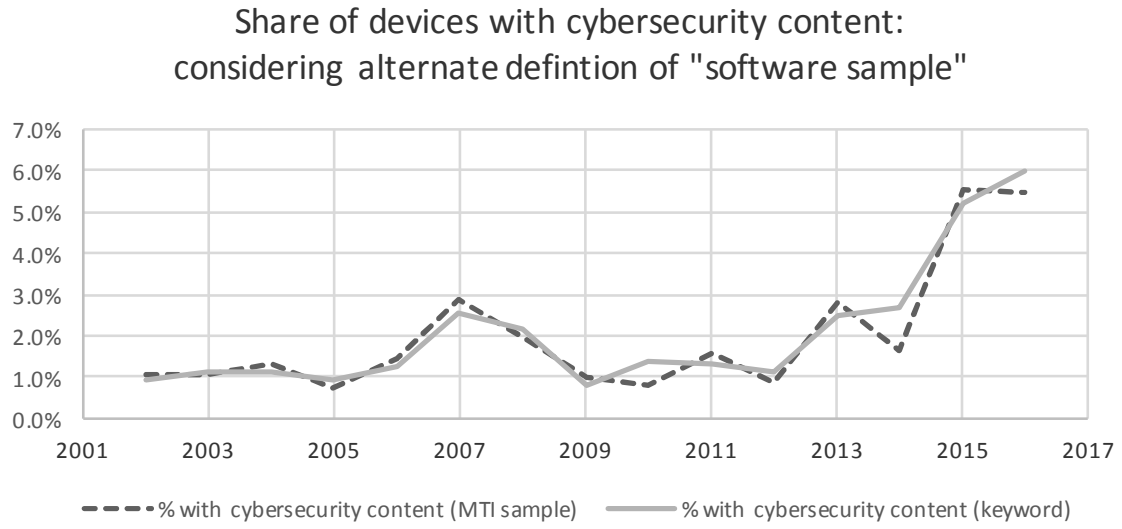
Indeed, the keyword-based method of identifying software products captured 100% of the products that were identified as including software using the MTI results, but also identified additional products that employ the word "software" in their product summaries at least once (**Supplementary Table**).

Relative to the keyword method, we conclude that the MTI-based method of identifying software products had a 100% sensitivity, but only a 94.8% specificity in our sample. Given the high sensitivity of this method, the MTI-based software sample is the more conservative method for identifying devices with software. However, alternative results using the keyword-based definition are highly similar to those obtained using the MTI-based definition. The total share of the software device sample that includes cybersecurity content is statistically indistinguishable in every year of the sample and visibly similar over time (**Supplementary Table and Supplementary Figure**)

Supplementary Table: Comparison of MTI and Keyword-based Methods of Identifying Software over Time

Year	Total Devices	Software sample (MTI defined)	Software sample (keyword defined)	Total devices with cybersecurity content (MTI)	% with cybersecurity content (MTI sample)	Total devices with cybersecurity content (keyword sample)	% with cybersecurity content (keyword)
2002	2573	275	318	3	1.09%	3	0.94%
2003	2565	289	347	3	1.04%	4	1.15%
2004	2476	298	350	4	1.34%	4	1.14%
2005	2338	277	323	2	0.72%	3	0.93%
2006	2430	339	397	5	1.47%	5	1.26%
2007	2245	276	314	8	2.90%	8	2.55%
2008	2333	309	371	6	1.94%	8	2.16%
2009	2287	303	373	3	0.99%	3	0.80%
2010	2168	254	356	2	0.79%	5	1.40%
2011	2405	380	524	6	1.58%	7	1.34%
2012	2466	357	526	3	0.84%	6	1.14%
2013	2404	395	597	11	2.78%	15	2.51%
2014	2509	421	635	7	1.66%	17	2.68%
2015	2334	361	636	20	5.54%	33	5.19%
2016	2261	402	721	22	5.47%	43	5.96%
Totals	35794	4936	6788	105	2.13%	164	2.42%

Supplementary Figure: comparison of main results using alternative method of identifying the software sample



List of keywords related to cybersecurity content:

Source	Term	Allowable alternative(s)
NICCS	access control	
NICCS	active attack	
NICCS	air gap	
NICCS	antispyware software	anti-spyware software, anti-spyware, antispyware
NICCS	antivirus software	anti-virus software, anti-virus, antivirus
NICCS	asymmetric cryptography	
NICCS	cipher	
NICCS	ciphertext	
NICCS	computer network defense	
NICCS	computer network defense analysis	
NICCS	computer network defense infrastructure support	
NICCS	computer security incident	
NICCS	cryptanalysis	
NICCS	cryptographic algorithm	
NICCS	cryptography	
NICCS	cyber ecosystem	
NICCS	cyber exercise	
NICCS	cyber incident	cyber-incident
NICCS	cyber incident response plan	
NICCS	cyber infrastructure	cyber-infrastructure
NICCS	cybersecurity	cyber-security
NICCS	data breach	
NICCS	data leakage	
NICCS	data theft	data-theft
NICCS	decrypt	
NICCS	decryption	
NICCS	denial of service	denial-of-service
NICCS	designed-in security	designed in security
NICCS	digital forensics	
NICCS	distributed denial of service	distributed denial-of-service, DDOS, D.D.O.S.
NICCS	dynamic attack surface	
NICCS	encrypt	
NICCS	encryption	
NICCS	enterprise risk management	
NICCS	exploitation analysis	
NICCS	hacker	hacking
NICCS	identity and access management	
NICCS	information security policy	
NICCS	information system resilience	
NICCS	Information Systems Security Operations	Information Systems Security
NICCS	intrusion detection	
NICCS	malicious code	
NICCS	malware	
NICCS	NICCS	National Initiative for Cybersecurity Careers and Study
NICCS	penetration testing	
NICCS	phishing	
NICCS	security incident	
NICCS	security policy	
NICCS	spyware	spy-ware
NICCS	symmetric cryptography	
NICCS	symmetric encryption algorithm	
NICCS	symmetric key	
NICCS	systems security architecture	
NICCS	threat assessment	
NICCS	virus	
FDA Guidance	cybersecurity routine updates and patches	cybersecurity routine updates, cybersecurity routine patches
FDA Guidance	cybersecurity signal	
FDA Guidance	exploit	
FDA Guidance	Information Sharing Analysis Organizations	ISAO, ISAOs
FDA Guidance	NIST	National Institute of Standards and Technology
FDA Guidance	NIST Framework	NIST Framework for Improving Critical Infrastructure Cybersecurity
FDA Guidance	Postmarket Management of Cybersecurity in Medical Devices	post-market management of cybersecurity in medical devices
FDA Guidance	Protected Critical Infrastructure Information	PCII

BMJ Open

Cybersecurity Features of Digital Medical Devices: An Analysis of FDA Product Summaries

Journal:	*BMJ Open*
Manuscript ID	bmjopen-2018-025374.R1
Article Type:	Research
Date Submitted by the Author:	08-Feb-2019
Complete List of Authors:	Stern, Ariel; Harvard Business School Technology and Operations Management; Harvard-MIT Center for Regulatory Science Gordon, William; Brigham and Women's Hospital Department of Medicine; Harvard Medical School Landman, Adam; Brigham and Women's Hospital Department of Medicine Kramer, Daniel; Beth Israel Deaconess Medical Center, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology; Harvard Medical School
Primary Subject Heading:	Health informatics
Secondary Subject Heading:	Health policy, Pharmacology and therapeutics
Keywords:	Medical Devices, Software, Cybersecurity, FDA, Regulatory Policy

CYBERSECURITY FEATURES OF DIGITAL MEDICAL DEVICES:

AN ANALYSIS OF FDA PRODUCT SUMMARIES

Ariel D Stern, Assistant Professor Harvard Business School and the Harvard-MIT Center for Regulatory Science, Morgan Hall 433, Soldiers Field Rd, Boston, MA 02163, astern@hbs.edu

William J Gordon, Instructor of Medicine, Division of General Internal Medicine, Brigham and Women's Hospital, Harvard Medical School, 1620 Tremont Street, Boston, MA 02120, wgordon@partners.org

Adam B Landman, Chief Information Officer, Brigham and Women's Hospital, Harvard Medical School, 75 Francis St, Boston, MA 02115, alandman@bwh.harvard.edu

Daniel B Kramer, Assistant Professor of Medicine, Harvard Medical School, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology, Beth Israel Deaconess Medical Center, Baker 4, West, 330 Brookline Ave, Boston, MA 02115, dkramer@bidmc.harvard.edu

Correspondence to: Ariel D Stern

Keywords: Medical Devices, Software, Cybersecurity, FDA

Word Count: 2522

Structured Abstract

Objectives: In order to more clearly define the landscape of digital medical devices subject to U.S. Food and Drug Administration (FDA) oversight, this analysis leverages publicly-available regulatory documents to characterize the prevalence and trends of software and cybersecurity features in regulated medical devices.

Design: We analyzed data from publicly available FDA product summaries to understand the frequency and recent time trends of inclusion of software and cybersecurity content in publicly available product information.

Setting: The full set of regulated medical devices, approved over the years 2002-2016 included in the FDA's 510(k) and premarket approval databases.

Primary and secondary outcome measures: The primary outcome was the share of devices containing software that included cybersecurity content in their product summaries. Secondary outcomes were differences in these shares a) over time and b) across regulatory areas.

Results: Among regulated devices, 13.79% were identified as including software. Among these products, only 2.13% had product summaries that included cybersecurity content over the period studied. The overall share of devices including cybersecurity content was higher in recent years, growing from an average of 1.4% in the first decade of our sample to 5.5% in 2015 and 2016, the most recent years included. The share of devices including cybersecurity content also varied across regulatory areas from a low of 0% to a high of 22.2%.

Conclusions: To ensure the safest possible health care delivery environment for patients and hospitals, regulators and manufacturers should work together to make the software and cybersecurity content of new medical devices more easily accessible.

Article Summary

Strengths and limitations of this study

- Cybersecurity issues related to medical devices have been documented in a number of individual cases, but the inclusion of cybersecurity content has never been considered systematically; we provide the first such analysis.
- The study also provides a new application of the use of the Medical Text Indexer – a document classification algorithm from the U.S. National Library of Medicine – for understanding the content of medical product descriptions.
- The study's primary limitation is that because the inclusion of cybersecurity content is not currently mandatory in FDA product summary documents, some devices may include cybersecurity features that cannot be accounted for by this analysis.

Introduction

The United States (US) National Research Council (NRC) defines cybersecurity as "the technologies, processes, and policies that help to prevent and/or reduce the negative impact of events…that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor."[1] In the US, the Cybersecurity Information Sharing Act of 2015 included health care provisions (Sec. 405), requiring the Department of Health and Human Services to report to Congress regarding the preparedness of the health care industry in responding to cybersecurity threats, acknowledging these risks and laying out reporting requirements.[2]

In health care delivery and health care policy, cybersecurity comes up most readily in the context of health information technology. Such technology may include stand-alone software, such as electronic health record systems, or combinations of hardware and software, such as those seen in modern pacemakers, blood glucose monitors, and computed tomography scanners. In the latter category, many digital products pose sufficient risk to patients as to require regulatory approval for use. In the US, products containing both software and hardware are regulated by the US Food and Drug Administration (FDA). Importantly, digital medical devices – those that contain software and/or digital networking capabilities – are quickly becoming embedded in all facets of medical care. However, the prevalence of software and the inclusion of cybersecurity features among already-marketed regulated medical devices have not been previously investigated.

At the same time, there have been several recent examples of software-related medical device vulnerabilities,[3,4] including potential use of a pacemaker remote monitoring system to issue malicious programming commands.[5] These devices may also place health care facilities at

risk:[6] A recent report from a cybersecurity firm highlighted the fact that 90% of hospitals had been targeted by cybercriminals in the past two years and that 17% of these documented attacks had been facilitated by Internet-connected medical devices.[7] The May 2017 WannaCry ransomware attack was the largest cyberattack to affect the United Kingdom's National Health Service, impacting 34% of trusts and disrupting some medical devices, including a subset of MRI scanners and devices to test blood and tissue samples.[8,9]

In recognition of these risks, the FDA has issued both pre and post-market regulatory guidance[10,11] on medical device cybersecurity while actively engaging industry and outside experts in addressing post-market cybersecurity concerns. In order to more clearly define the landscape of digital medical devices subject to FDA oversight, this analysis leverages publicly-available FDA documents to characterize the prevalence and trends of software and cybersecurity features in regulated medical devices.

Methods

Data Sources

We analyzed data from publicly available FDA product summaries, identified from searchable documents published by the FDA at the time of each new device's clearance or approval for marketing.[12,13] Such summaries have supported previous analyses,[14,15] and, as outlined by FDA guidance, these summaries contain information such as indications for use, a detailed device description (including device design, material use, and physical properties), contradictions/warnings/precautions, and clinical evidence supporting the regulatory assessment of safety and effectiveness.[16,17] Along with the FDA-approved product label (with which a summary will share many pieces of important information), summary documents represent key

pieces of publicly available information about medical devices that have been granted marketing approval or clearance in the United States.

We used the FDA's 510(k) and premarket approval (PMA) databases to identify all new device clearances and approvals from 2002-2016, respectively[14,15] (see **Table 1** in the **Supplementary Material**). In brief, under the FDA's risk-based framework for premarket evaluation, high-risk devices are evaluated under the PMA pathway, which includes demonstration of clinically-relevant safety and effectiveness. By contrast, medium-risk devices are generally assessed via the "510k" pathway, which evaluates whether new safety or effectiveness concerns are raised by the device at issue compared to a "substantially equivalent" device already on the market.[18,19] **Figure 1** of the **Supplementary Material** presents a brief overview of these pathways and their typical components. We identified the eight largest medical device categories by advisory committee of assignment. Advisory committees correspond largely to medical specialties (e.g. committees exist for cardiovascular, radiological, and orthopedic devices) and the eight largest committees accounted for over 75%[14,15] of all regulated devices that came to market over this period of time (see **Figure 1** for a summary of how the analysis sample was identified). Modifications to already-marketed devices approved via the "PMA supplement" pathway[20] were excluded.

We used an automated script to batch download all associated product summaries and applied *ABBYY FineReader* optical character recognition software (ABBYY, Milpitas, CA) to convert these Portable Document Format (PDF) files into machine-readable text files.

Analysis Sample

We used the US National Institute of Health's National Library of Medicine (NLM) *Medical Text Indexer*[21] (MTI) to identify digital devices as those referencing and/or describing software in their product summaries. The MTI uses natural language processing algorithms that take free text as input and provide medical subject indexing recommendations, based on the MeSH® vocabulary[22] established by the NLM, as output. From a regulatory perspective, products containing software must describe this in their summaries (see above). Indeed, many device summaries contain a short section of the document that is dedicated to describing the product's software (for example, as seen for the Medtronic MiniMed 670G Automated Insulin Delivery System).[23] We used the sample of summaries that were flagged by the MTI as including the medical subject of "software" as our analysis sample of digital devices ("software sample"). In sensitivity analysis, an alternative, keyword-based definition was considered and did not impact findings (**Table 1 and Figure 2 of Supplementary Material**). For each product in the software sample, we recorded each device's FDA decision date (i.e. the year in which the product came to market), its regulatory approval pathway (510(k) or PMA), and the reviewing advisory committee.

Characterization of Cybersecurity Features

The "cybersecurity features" of digital medical devices can take on a number of forms, each of which can address the risks of actions by malevolent parties. Such cybersecurity features may include characterizations or descriptions of a digital product's defensive abilities (e.g. data encryption), an ability to respond to a security breach should it be attempted (e.g. antivirus software), or the ability to detect a breach that has already occurred (e.g. penetration testing).

We searched each of the summaries in the software sample for a pre-specified list of keywords related to cybersecurity content (**Table 2 of Supplementary Material**) and documented use of these keywords (yes/no) in each product summary. These keywords and phrases were selected *a priori* from terminology glossaries from the US National Initiative for Cybersecurity Careers and Studies (NICCS), the FDA's guidance on cybersecurity for medical devices, the US National Institute of Standards and Technology (NIST 4009 / NISTIR 7298) Glossary,[24] and the Manufacturer Disclosure Statement for Medical Device Security (MDS2), a multi-stakeholder devised form designed to give manufacturers a mechanism of disclosing security-related product information to healthcare providers.[25]

Patient and Public Involvement

Patients were not directly involved in the design of this retrospective study of publicly-available regulatory documents. However, popular media accounts of recent cybersecurity concerns in medical devices has brought this previously-obscure topic to the attention of a wide public audience, particularly the millions of patients living with potentially affected devices.[26–28]

Data Analysis

For each year, we identified the software sample and calculated the number and percentage (share) of devices that included cybersecurity content by advisory committee and overall. We compared the percentage of devices with cybersecurity content, as identified by keywords. Using chi-squared tests, we looked at differences between the two major regulatory approval pathways and in earlier versus later years.

In order to validate our automated search protocol, we manually reviewed 100 summaries. We selected 50 summaries from the software sample that were identified as containing cybersecurity information, and 50 that were identified as having no such content to confirm text scraping methods. Discrepancies were reviewed by group assent. We further validated our method of identifying devices containing software by electronically scanning all product summaries for the keyword "software" and using these results to assess the sensitivity and specificity of the MTI-defined software sample. (**Supplementary Material**).

All statistical analyses were conducted in STATA version 14.2 (StataCorp LLC, College Station, TX).

Results

A total of 36,430 new devices were identified (**Figure 1**) and of those, 35,794 (98.3%) had product summaries that could be converted to machine-readable text. From this sample, 4,936 new devices (13.79%) were identified by the MTI as including software (9.70% of PMA devices and 13.82% of 510(k) devices. Within the software sample, we found that only 2.13% of devices had product summaries that included cybersecurity content (3.45% of PMA devices and 2.12% of 510(k) devices included cybersecurity content in their summaries, however, differences between PMA and 510(k) devices were not statistically significant [p=0.62]). Manual review confirmed that 100% of summaries included the keyword(s) found by our automated program. Relative to our keyword-based validation exercise, the MTI had a sensitivity of 100% and a specificity of 94.8%, making it a more conservative measure.

Figure 2 presents the share of devices with software over time, while **Figure 3** presents the share of devices in the software sample that included cybersecurity content in their product

summaries over the same period. The overall share of devices including cybersecurity content was higher in recent years, growing from an average of 1.4% in the first decade of our sample to an average of 5.5% in 2015 and 2016, the most recent years included in the sample ($p = 0.0181$). The share of devices including cybersecurity content also varied across regulatory areas from a low of 0% across all years in gastroenterology/urology devices, orthopedic devices, and general/plastic surgery devices, to a high of 22.2% among general hospital devices in 2016 (**Table 1**). **Supplementary Table 2** provides additional detail of the frequencies of individual keywords in the sample.

Discussion

Summary

This study leverages a novel methodology to create an analyzable dataset from public documents describing newly-marketed medical devices. We found that software is an increasingly common component of newly approved or cleared devices, while cybersecurity content in the devices' publicly available product summaries remains rare.

As more and more aspects of healthcare are digitized, the cybersecurity of our healthcare infrastructure—including medical devices—will be increasingly essential to delivering safe and effective care. Recent events such as the emergence of pacemaker vulnerabilities have highlighted both the public health implications of information security[29] and importance of device security.[6] Additionally, the recent security flaws discovered in widely-used computer processors, highlight the fact that new threats continue to emerge[30] and scholars have highlighted medicine as a domain where adversarial attacks may be particularly likely to unfold,[31] with the opportunity for significant clinical impact. Indeed, the NRC has written that "from the standpoint

of an individual system or network operator, the only thing worse than being penetrated is being penetrated and not knowing about it."[1] This study is an important first step in understanding the public, transparent reporting of cybersecurity features included in the software embedded in moderate- and high-risk medical devices. Indeed, our characterization of the growing importance of software among medium- and high-risk devices should encourage policy-makers to buttress FDA's resources accordingly, including support for partnerships with the Department of Homeland Security and other government, academic, and industry partners focused on anticipating and responding to emerging threats to patients and public health.

Limitations

The key limitation of this study is that the information we collected is not a mandatory component of the documents considered. As a result, product summaries may not include all relevant details of a device's design with respect to cybersecurity. While this information may have been present in other places, such as proprietary applications or the full, confidential FDA dossier, device summaries represent some of the primary documents available for public review, and therefore play an important role in educating stakeholders, such as clinicians, purchasing managers, patients, and administrators of health care systems, about the strength of safety and effectiveness evidence when a new product comes to market. The potential for unobserved information related to cybersecurity content is the key weakness of this study, however the study's key strength is that it is, to our knowledge, the first to take a large-scale approach to characterizing the availability of cybersecurity content among approved medical devices.

Policy Implications

These findings help define the current landscape of medical device software and cybersecurity features, and suggest an opportunity to better inform healthcare professionals, those engaging in device procurement on behalf of hospitals and health care systems, and patients, on the cybersecurity protections embedded in medical devices. In particular, the current FDA Commissioner, Dr. Scott Gottlieb, has publicly acknowledged the importance of the availability of cyber security information, noting that "Securing medical devices from cybersecurity threats cannot be achieved by just the FDA alone" and that "every stakeholder – manufacturers, hospitals, health care providers, cybersecurity researchers and gov[ernment] entities [has] a unique role to play in addressing these modern challenges."[32] In the fourth quarter of 2018, in response to the need to "ensure the health care sector is well positioned to proactively respond when cyber vulnerabilities are identified,"[33] the FDA released updated guidance on the content of premarket submissions for the management of cybersecurity in medical devices[10] and the U.S. Department of Health and Human Services similarly recently released voluntary guidance on cybersecurity practices for healthcare organizations[34]. Ongoing opportunities for the exchange of ideas and best practices among regulators, practitioners, and cybersecurity experts, such as those recently hosted by the FDA on the "management of cybersecurity in medical devices"[35] and collaborations between the security research and medical device communities[36] will be valuable for ensuring public health and a better-informed public and medical community will be crucial to ensuring the safety of medical devices moving forward.

Our findings also support the case for recent proposals by US regulators to include a cybersecurity "bill of materials" in the submission of new medical devices. The proposal calls for "principles and approaches [that] are broadly applicable to all medical devices and are intended to be consistent with the National Institute of Standards and Technology (NIST)

Framework for Improving Critical Infrastructure Cybersecurity."[10] Such a standardized approach would represent an important step in addressing the cybersecurity information deficit that we have documented here. Further, many individual hospitals and other purchasers of medical devices currently perform independent information security assessments of medical devices - a slow, resource intensive, and costly process. Standardizing the information security review process and making the results available publicly would bring substantial efficiencies for medical device vendors and healthcare organizations.

Looking Ahead

In an increasingly digitized health care ecosystem, manufacturers will face increasing demands for product safety in the form of cybersecurity protections. Moreover, stakeholders will increasingly seek out information about the safety features of new products. Regulators and manufacturers should collaborate to make the software and cybersecurity content of new products more easily accessible, and should continue to work together to determine which cybersecurity content should be disclosed and required for regulatory clearance and approval of new products moving forward. It will also be important for future researchers to closely track the availability of cybersecurity content in newly-approved medical devices and to explore whether the publication of such content impacts the product utilization decisions of patients and health care providers.

Figure Legend

Figure 1: Assembly of analysis sample and results

Figure 2: Share of new devices with software ("software sample")

Figure 3: Share of software sample with cybersecurity content

Author Contributions: ADS designed the study in consultation with WJG, ABL, and DBK. ADS collected the data from public sources and performed the primary analysis. All authors had full access to the data and analysis programs for this study and take responsibility for the integrity of the data and the accuracy of the analysis. All authors wrote the manuscript.

Data Sharing Statement: Statistical code and the full dataset are available at https://github.com/arieldora/SternCybersecurityContent

Conflicts of Interest: Dr. Landman is a member of the Abbott Medical Device Cybersecurity Council. Dr. Kramer is supported by the Greenwall Faculty Scholars Program in Bioethics, is a consultant to Circulatory Systems Advisory Panel of the Food and Drug Administration, and has provided consulting to the Baim Institute for Clinical Research for clinical trials of medical devices (unrelated to the study topic). There are no other financial or commercial financial conflicts of interest related to the study topic to report.

Funding: The Harvard Business School Division of Research and Faculty Development supported the data collection for this study. Dr. Stern is supported by the Kauffman Junior

Faculty Fellowship and Dr. Kramer is supported by the Greenwall Faculty Scholars Program in Bioethics.

References

1. National Research Council. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues [Internet]. The National Academies Press; 2014. Available from: https://doi.org/10.17226/18749 [accessed 10 Jul 2018].

2. Burr R. S.754 - 114th Congress (2015-2016): To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. [Internet]. 2015. Available from: https://www.congress.gov/bill/114th-congress/senate-bill/754 [accessed 10 Jul 2018].

3. Blau M. Hospitals brace for security risks that could come with using wearables for patient care [Internet]. STAT. 2017. Available from: https://www.statnews.com/2017/08/04/hospitals-security-risks-wearables/ [accessed 10 Jul 2018].

4. Kuchler H. Medical device makers wake up to cyber security threat. Financial Times [Internet]. 2017 Aug 1; Available from: https://www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691 [accessed 10 Jul 2018].

5. Kramer DB, Fu K. Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. JAMA. 2017 Dec 5;318(21):2077–8.

6. Fox-Brewster T. Medical Devices Hit By Ransomware For The First Time In US Hospitals [Internet]. Forbes. 2017. Available from: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4a76dbe8425c [accessed 10 Jul 2018].

7. IoT guardian for the healthcare industry [Internet]. ZingBox; 2016. Available from: http://www.zingbox.com/wp-content/uploads/2017/02/ZingBox_WP_IoT-Guardian-for-the-Healthcare-Industry.pdf [accessed 10 Jul 2018].

8. Hughes O. WannaCry impact on NHS considerably larger than previously suggested [Internet]. Digital Health. 2017. Available from: https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/ [accessed 10 Jul 2018].

9. Department of Health. Investigation: WannaCry cyber attack and the NHS [Internet]. 2017 Oxtober. Report No.: HC 414. Available from: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [accessed 10 Jul 2018].

10. Food and Drug Administration. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff. Available from: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [accessed 10 Jul 2018].

11. Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff. Available from:

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf [accessed 10 Jul 2018].

12. 510(k) Premarket Notification. 2017; Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPMN/pmn.cfm [accessed 10 Jul 2018].

13. Premarket Approval (PMA). 2018; Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPMA/pma.cfm [accessed 10 Jul 2018].

14. Zheng SY, Dhruva SS, Redberg RF. Characteristics of Clinical Studies Used for US Food and Drug Administration Approval of High-Risk Medical Device Supplements. JAMA. 2017 Aug 15;318(7):619–25.

15. Dhruva SS, Bero LA, Redberg RF. Strength of study evidence examined by the FDA in premarket approval of cardiovascular devices. JAMA. 2009 Dec 23;302(24):2679–85.

16. Content of a 510(k). 2017 Oct 31; Available from: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/ucm142651.htm#link_7 [accessed 10 Jul 2018].

17. PMA Application Contents. 2018 Feb 2; Available from: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm050289.htm#ssed [accessed 10 Jul 2018].

18. Kramer DB, Kesselheim AS. User Fees and Beyond — The FDA Safety and Innovation Act of 2012. N Engl J Med. 2012 Oct 4;367(14):1277–9.

19. Kramer DB, Xu S, Kesselheim AS. Regulation of Medical Devices in the United States and European Union. N Engl J Med. 2012 Mar 1;366(9):848–55.

20. Rome BN, Kramer DB, Kesselheim AS. FDA approval of cardiac implantable electronic devices via original and supplement premarket approval pathways, 1979-2012. JAMA. 2014 Jan 22;311(4):385–91.

21. NLM Medical Text Indexer (MTI). 2018; Available from: https://ii.nlm.nih.gov/MTI [accessed 10 Jul 2018].

22. MeSH [Internet]. [cited 2018 Feb 5]. Available from: https://www.ncbi.nlm.nih.gov/mesh [accessed 10 Jul 2018].

23. Summary of Safety and Effectiveness Data (SSED) [Internet]. Available from: https://www.accessdata.fda.gov/cdrh_docs/pdf10/P100034b.pdf [accessed 10 Jul 2018].

24. Kissel R. Glossary of Key Information Security Terms [Internet]. 2013 p. 1–218. Available from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [accessed 10 Jul 2018].

25. Manufacturer Disclosure Statement for Medical Device Security (MDS2). 2017; Available from: http://www.himss.org/resourcelibrary/MDS2 [accessed 10 Jul 2018].

26. How medical devices like pacemakers and insulin pumps can be hacked [Internet]. CBS News. Available from: https://www.cbsnews.com/news/cybersecurity-researchers-show-medical-devices-hacking-vulnerabilities/ [accessed 29 Jan 2019].

27. Gellman L. Insecure Medical Devices Vulnerable to Malicious Hacking [Internet]. Available from: http://nymag.com/intelligencer/2018/08/insecure-medical-devices-vulnerable-to-malicious-hacking.html [accessed 29 Jan 2019].

28. Innes S. “Ethical hackers” are working to warn physicians about cyberattacks [Internet]. 2018. Available from: https://www.azcentral.com/story/news/local/arizona-health/2018/12/27/ethical-hackers-warn-physicians-cyberattacks-christian-dameff-arizona-college-medicine-jeff-tully/2277625002/ [accessed 29 Jan 2019].

29. Gordon WJ, Fairhall A, Landman A. Threats to Information Security — Public Health Implications. N Engl J Med. 2017 Aug 24;377(8):707–9.

30. Finlayson SG, Won Chung H, Kohane IS, Beam AL. Adversarial Attacks Against Medical Deep Learning Systems. arXiv [Internet]. 2018 May 21 [cited 2019 Jan 31]; Available from: https://arxiv.org/abs/1804.05296 [accessed 29 Jan 2019].

31. Metz C, Perlroth N. Researchers Discover Two Major Flaws in the World’s Computers. The New York Times [Internet]. 2018 Jan 3; Available from: https://www.nytimes.com/2018/01/03/business/computer-flaws.html [accessed 10 Jul 2019].

32. Scott Gottlieb, M.D. on Twitter: “4/4 Securing medical devices from cybersecurity threats cannot be achieved by just the #FDA alone. Every stakeholder—manufacturers, hospitals, health care providers, cybersecurity researchers and govt entities – all have a unique role to play in addressing these modern challenges” [Internet]. 2018. Available from: https://twitter.com/SGottliebFDA/status/1046847875840450560 [accessed 29 Jan 2019].

33. FDA In Brief: FDA proposes updated cybersecurity recommendations to help ensure device manufacturers are adequately addressing evolving cybersecurity threats [Internet]. 2018. Available from: https://www.fda.gov/NewsEvents/Newsroom/FDAInBrief/ucm623624.htm [accessed 29 Jan 2019].

34. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. 36. Available from: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf [accessed 29 Jan 2019].

35. Workshops & Conferences (Medical Devices) > Public Workshop - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices January 29-30, 2019 [Internet]. Available from: https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm623171.htm [accessed 29 Jan 2019].

36. #WeHeartHackers | A collaborative movement between the medical device and security researcher communities. [Internet]. [cited 2019 Jan 31]. Available from: http://wehearthackers.org/ [accessed 29 Jan 2019].

Table 1: Number of devices with machine-readable summaries by FDA/CDRH Advisory Committee and year, share with software and share of software sample with cybersecurity content by Advisory Committee

	FDA/CDRH Advisory Committee								
Year	Clinical Chemistry (CH)	Cardiovascular (CV)	Dental (DE)	Gastroenterology, Urology (GU)	General Hospital (HO)	Orthopedic (OR)	Radiology (RA)	General, Plastic Surgery (SU)	Totals
2002	216	436	318	215	328	403	290	367	2573
2003	192	441	295	233	329	389	329	357	2565
2004	204	395	284	195	270	464	345	319	2476
2005	155	389	245	166	262	480	310	331	2338
2006	197	412	293	142	244	442	338	362	2430
2007	153	358	283	160	257	444	271	319	2245
2008	149	387	279	139	207	477	325	370	2333
2009	130	442	268	155	254	432	290	316	2287
2010	121	390	245	157	280	428	235	312	2168
2011	163	428	258	141	241	542	347	285	2405
2012	155	426	240	166	282	551	344	302	2466
2013	185	428	235	153	202	554	346	301	2404
2014	130	400	225	199	245	583	385	342	2509
2015	108	392	244	179	174	575	340	322	2334
2016	95	368	230	171	204	464	375	354	2261
Totals	2353	6092	3942	2571	3779	7228	4870	4959	35794
Share with software ("software sample")	9.14%	18.99%	4.59%	8.01%	4.97%	1.36%	52.28%	6.96%	13.79%
Share of software sample with cybersecurity content	7.91%	2.51%	1.66%	0.00%	2.13%	0.00%	2.04%	0.00%	2.13%

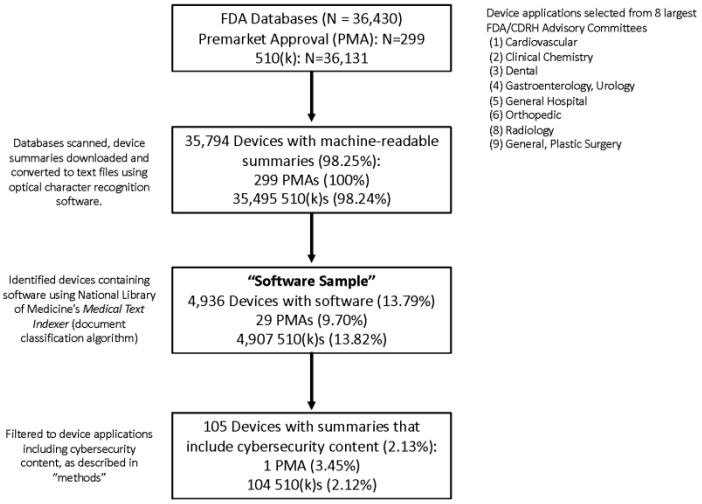


Figure 1: Assembly of analysis sample and results

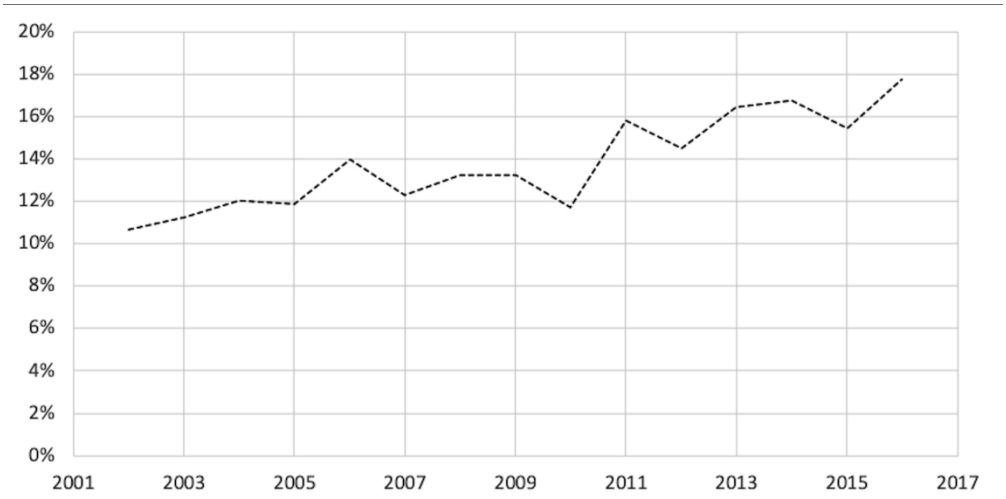


Figure 2: Share of new devices with software ("software sample")

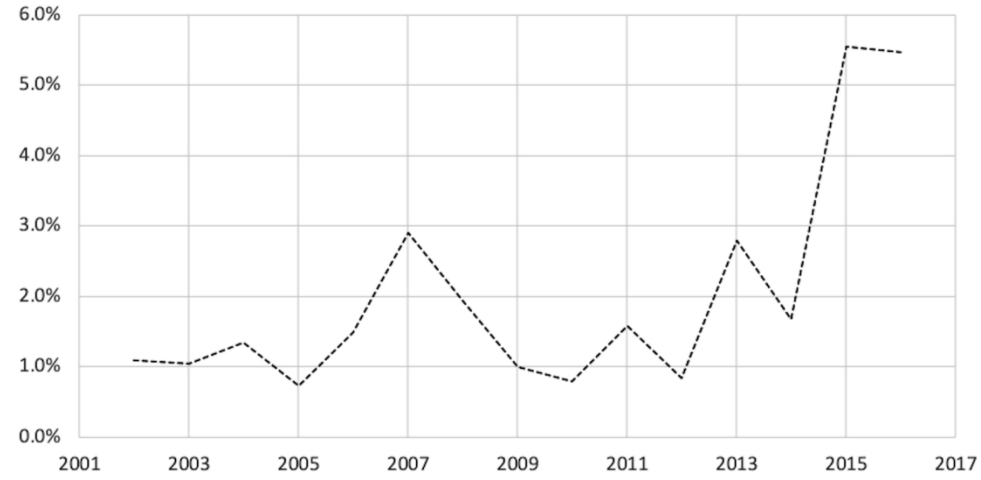


Figure 3: Share of software sample with cybersecurity content

Supplementary Material

I. Processing Using the Medical Text Indexer (MTI)

We sent each of our optical character recognition-processed text files to the MTI and recorded which summaries were classified as being related to software In the MeSH® Tree (ontology). We flagged all products whose summaries were assigned to the "software" MeSH® term, number L01.224.900.

II. Sensitivity Analysis

In sensitivity analyses we considered an alternate method of identifying devices containing software. For this exercise, we electronically scanned each product summary for the keyword "software" and recorded whether the word "software" appeared anywhere within a device's product summary (i.e. at least once in the document).

We expected that the MTI-driven method of identifying the "software sample" would have a high sensitivity but a lower specificity relative to the keyword-based method for the following reason: in order for a text document to be flagged by the MTI's algorithm as being related to the subject of "software" the text document would need describe relevant software content in some detail – i.e. often beyond simply utilizing the keyword "software" at least once.

Indeed, the keyword-based method of identifying software products captured 100% of the products that were identified as including software using the MTI results, but also identified additional products that employ the word "software" in their product summaries at least once (**Supplementary Table**).

Relative to the keyword method, we conclude that the MTI-based method of identifying software products had a 100% sensitivity, but only a 94.8% specificity in our sample. Given the high sensitivity of this method, the MTI-based software sample is the more conservative method for identifying devices with software. However, alternative results using the keyword-based definition are highly similar to those obtained using the MTI-based definition. The total share of the software device sample that includes cybersecurity content is statistically indistinguishable in every year of the sample and visibly similar over time (**Supplementary Table and Supplementary Figure**)

Supplementary Table 1: Comparison of MTI and Keyword-based Methods of Identifying Software over Time

Year	Total Devices	Software sample (MTI defined)	Software sample (keyword defined)	Total devices with cybersecurity content (MTI)	% with cybersecurity content (MTI sample)	Total devices with cybersecurity content (keyword sample)	% with cybersecurity content (keyword)
2002	2573	275	318	3	1.09%	3	0.94%
2003	2565	289	347	3	1.04%	4	1.15%
2004	2476	298	350	4	1.34%	4	1.14%
2005	2338	277	323	2	0.72%	3	0.93%
2006	2430	339	397	5	1.47%	5	1.26%
2007	2245	276	314	8	2.90%	8	2.55%
2008	2333	309	371	6	1.94%	8	2.16%
2009	2287	303	373	3	0.99%	3	0.80%
2010	2168	254	356	2	0.79%	5	1.40%
2011	2405	380	524	6	1.58%	7	1.34%
2012	2466	357	526	3	0.84%	6	1.14%
2013	2404	395	597	11	2.78%	15	2.51%
2014	2509	421	635	7	1.66%	17	2.68%
2015	2334	361	636	20	5.54%	33	5.19%
2016	2261	402	721	22	5.47%	43	5.96%
Totals	35794	4936	6788	105	2.13%	164	2.42%

Supplementary Table 2: List of keywords related to cybersecurity content:

Source	Term	Allowable alternative(s)	Counts
NICCS	access control		17
NICCS	active attack		0
NICCS	air gap		5
NICCS	antispyware software	anti-spyware software, anti-spyware, antispyware	1
NICCS	antivirus software	anti-virus software, anti-virus, antivirus	3
NICCS	asymmetric cryptography		0
NICCS	cipher		0
NICCS	computer network defense		0
NICCS	computer security incident		0
NICCS	cryptanalysis		0
NICCS	cryptographic algorithm		0
NICCS	cryptography		1
NICCS	cyber ecosystem		0
NICCS	cyber exercise		0
NICCS	cyber incident	cyber-incident	0
NICCS	cyber infrastructure	cyber-infrastructure	0
NICCS	cybersecurity	cyber-security	58
NICCS	data breach		0
NICCS	data leakage		0
NICCS	data theft	data-theft	0
NICCS	decrypt		3
NICCS	denial of service	denial-of-service	0
NICCS	designed-in security	designed in security	0
NICCS	digital forensics		0
NICCS	distributed denial of service	distributed denial-of-service, DDOS, D.D.O.S.	0
NICCS	dynamic attack surface		0

NICCS	encrypt		44
NICCS	enterprise risk management		0
NICCS	exploitation analysis		0
NICCS	identity and access management		0
NICCS	information security policy		0
NICCS	information system resilience	Information Systems Security	0
NICCS	Information Systems Security Operations		0
NICCS	intrusion detection		0
NICCS	malicious code		0
NICCS	malware		0
NICCS	NICCS	National Initiative for Cybersecurity Careers and Study	0
NICCS	penetration testing		83
NICCS	phishing		0
NICCS	security incident		0
NICCS	security policy		0
NICCS	spyware	spy-ware	0
NICCS	symmetric cryptography		0
NICCS	symmetric encryption algorithm		0
NICCS	symmetric key		0
NICCS	systems security architecture		0
NICCS	threat assessment		0
FDA Guidance	cybersecurity routine updates and patches	cybersecurity routine updates, cybersecurity routine patches	0
FDA Guidance	cybersecurity signal		0
FDA Guidance	exploit		2
FDA Guidance	Information Sharing Analysis Organizations	ISAO, ISAOs	2
FDA Guidance	NIST	National Institute of Standards and Technology	150
FDA Guidance	NIST Framework	NIST Framework for Improving Critical Infrastructure Cybersecurity	0

Supplementary Figure 1: FDA medical device approval pathways

	Regulatory Pathways for Medical Devices in the United States	
Pathway	510(k) (Premarket Notification)	PMA (Premarket Approval)
Products	Typically moderate-risk ("class II") devices	Typically high-risk ("class III") devices
Requirements	Typically do not necessitate full clinical trials, but require evidence of "substantial equivalence" to a predicate device, which has been shown to be safe and effective.	Typically require clinical trials to demonstrate a new device's safety and effectiveness
Product develompent time to market	31 months	54 months

Sources:

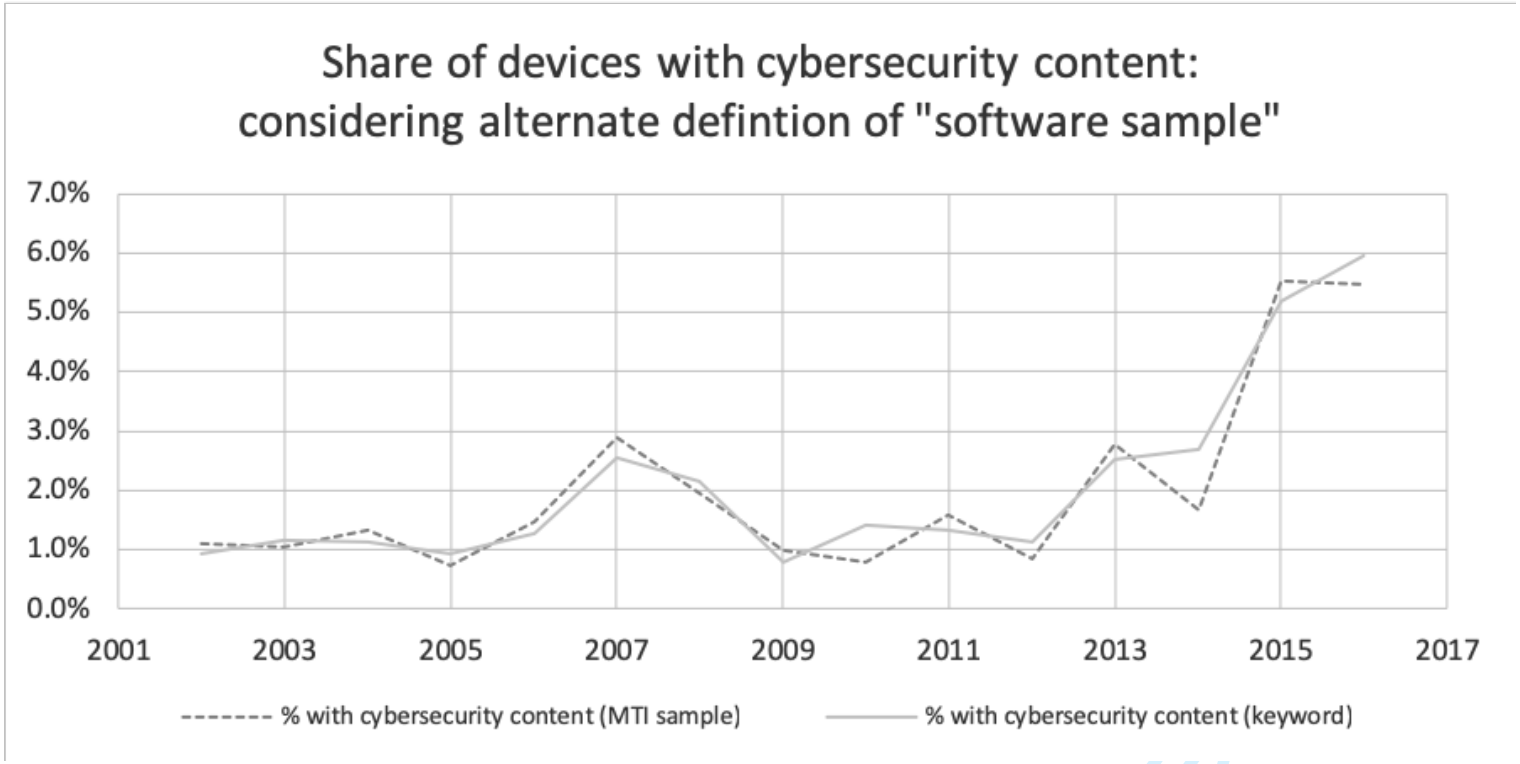
Maisel WH. Medical device regulation: an introduction for the practicing physician. Annals of internal medicine. 2004 Feb 17;140(4):296-302.

https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k

https://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/premarketsubmissions/premarketapprovalpma

Makower J, Meer A, Denend L. FDA impact on US medical technology innovation: a survey of over 200 medical technology companies. Advanced Medical Technology Association, Washington, DC, available at: http://www. advamed. org/NR/rdonlyres/040E6C33-380B-4F6B-AB58-9AB1C0A7A3CF/0/makowerreportfinal. pdf. 2010 Nov.

Supplementary Figure 2: comparison of main results using alternative method of identifying the software sample



BMJ Open

Cybersecurity Features of Digital Medical Devices: An Analysis of FDA Product Summaries

Journal:	*BMJ Open*
Manuscript ID	bmjopen-2018-025374.R2
Article Type:	Research
Date Submitted by the Author:	16-May-2019
Complete List of Authors:	Stern, Ariel; Harvard Business School Technology and Operations Management; Harvard-MIT Center for Regulatory Science Gordon, William; Brigham and Women's Hospital Department of Medicine; Harvard Medical School Landman, Adam; Brigham and Women's Hospital Department of Medicine Kramer, Daniel; Beth Israel Deaconess Medical Center, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology; Harvard Medical School
Primary Subject Heading:	Health informatics
Secondary Subject Heading:	Health policy, Pharmacology and therapeutics
Keywords:	Medical Devices, Software, Cybersecurity, FDA, Regulatory Policy

CYBERSECURITY FEATURES OF DIGITAL MEDICAL DEVICES:

AN ANALYSIS OF FDA PRODUCT SUMMARIES

Ariel D Stern, Assistant Professor Harvard Business School and the Harvard-MIT Center for Regulatory Science, Morgan Hall 433, Soldiers Field Rd, Boston, MA 02163, astern@hbs.edu

William J Gordon, Instructor of Medicine, Division of General Internal Medicine, Brigham and Women's Hospital, Harvard Medical School, 1620 Tremont Street, Boston, MA 02120, wgordon@partners.org

Adam B Landman, Chief Information Officer, Brigham and Women's Hospital, Harvard Medical School, 75 Francis St, Boston, MA 02115, alandman@bwh.harvard.edu

Daniel B Kramer, Assistant Professor of Medicine, Harvard Medical School, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology, Beth Israel Deaconess Medical Center, Baker 4, West, 330 Brookline Ave, Boston, MA 02115, dkramer@bidmc.harvard.edu

Correspondence to: Ariel D Stern

Keywords: Medical Devices, Software, Cybersecurity, FDA

Word Count: 2673

Structured Abstract

Objectives: In order to more clearly define the landscape of digital medical devices subject to U.S. Food and Drug Administration (FDA) oversight, this analysis leverages publicly-available regulatory documents to characterize the prevalence and trends of software and cybersecurity features in regulated medical devices.

Design: We analyzed data from publicly available FDA product summaries to understand the frequency and recent time trends of inclusion of software and cybersecurity content in publicly available product information.

Setting: The full set of regulated medical devices, approved over the years 2002-2016 included in the FDA's 510(k) and premarket approval databases.

Primary and secondary outcome measures: The primary outcome was the share of devices containing software that included cybersecurity content in their product summaries. Secondary outcomes were differences in these shares a) over time and b) across regulatory areas.

Results: Among regulated devices, 13.79% were identified as including software. Among these products, only 2.13% had product summaries that included cybersecurity content over the period studied. The overall share of devices including cybersecurity content was higher in recent years, growing from an average of 1.4% in the first decade of our sample to 5.5% in 2015 and 2016, the most recent years included. The share of devices including cybersecurity content also varied across regulatory areas from a low of 0% to a high of 22.2%.

Conclusions: To ensure the safest possible health care delivery environment for patients and hospitals, regulators and manufacturers should work together to make the software and cybersecurity content of new medical devices more easily accessible.

Article Summary

Strengths and limitations of this study

- Cybersecurity issues related to medical devices have been documented in a number of individual cases, but the inclusion of cybersecurity content has never been considered systematically; we provide the first such analysis.
- The study also provides a new application of the use of the Medical Text Indexer – a document classification algorithm from the U.S. National Library of Medicine – for understanding the content of medical product descriptions.
- The study's primary limitation is that because the inclusion of cybersecurity content is not currently mandatory in FDA product summary documents, some devices may include cybersecurity features that cannot be accounted for by this analysis.

Introduction

The United States (US) National Research Council (NRC) defines cybersecurity as "the technologies, processes, and policies that help to prevent and/or reduce the negative impact of events…that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor."[1] In the US, the Cybersecurity Information Sharing Act of 2015 included health care provisions (Sec. 405), requiring the Department of Health and Human Services to report to Congress regarding the preparedness of the health care industry in responding to cybersecurity threats, acknowledging these risks and laying out reporting requirements.[2]

In health care delivery and health care policy, cybersecurity comes up most readily in the context of health information technology. Such technology may include stand-alone software, such as electronic health record systems, or combinations of hardware and software, such as those seen in modern pacemakers, blood glucose monitors, and computed tomography scanners. In the latter category, many digital products pose sufficient risk to patients as to require regulatory approval for use. In the US, products containing both software and hardware are regulated by the US Food and Drug Administration (FDA). Importantly, digital medical devices – those that contain software and/or digital networking capabilities – are quickly becoming embedded in all facets of medical care. However, the prevalence of software and the inclusion of cybersecurity features among already-marketed regulated medical devices have not been previously investigated.

At the same time, there have been several recent examples of software-related medical device vulnerabilities,[3,4] including potential use of a pacemaker remote monitoring system to issue malicious programming commands.[5] These devices may also place health care facilities at

risk:[6] A recent report from a cybersecurity firm highlighted the fact that 90% of hospitals had been targeted by cybercriminals in the past two years and that 17% of these documented attacks had been facilitated by Internet-connected medical devices.[7] The May 2017 WannaCry ransomware attack was the largest cyberattack to affect the United Kingdom's National Health Service, impacting 34% of trusts and disrupting some medical devices, including a subset of MRI scanners and devices to test blood and tissue samples.[8,9]

In recognition of these risks, the FDA has issued both pre and post-market regulatory guidance[10,11] on medical device cybersecurity while actively engaging industry and outside experts in addressing post-market cybersecurity concerns. In order to more clearly define the landscape of digital medical devices subject to FDA oversight, this analysis leverages publicly-available FDA documents to characterize the prevalence and trends of software and cybersecurity features in regulated medical devices.

Methods

Data Sources

We analyzed data from publicly available FDA product summaries, identified from searchable documents published by the FDA at the time of each new device's clearance or approval for marketing.[12,13] Such summaries have supported previous analyses,[14,15] and, as outlined by FDA guidance, these summaries contain information such as indications for use, a detailed device description (including device design, material use, and physical properties), contradictions/warnings/precautions, and clinical evidence supporting the regulatory assessment of safety and effectiveness.[16,17] Along with the FDA-approved product label (with which a summary will share many pieces of important information), summary documents represent key

pieces of publicly available information about medical devices that have been granted marketing approval or clearance in the United States.

We used the FDA's 510(k) and premarket approval (PMA) databases to identify all new device clearances and approvals from 2002-2016, respectively[14,15] (see **Table 1** in the **Supplementary Material**). In brief, under the FDA's risk-based framework for premarket evaluation, high-risk devices are evaluated under the PMA pathway, which includes demonstration of clinically-relevant safety and effectiveness. By contrast, medium-risk devices are generally assessed via the "510k" pathway, which evaluates whether new safety or effectiveness concerns are raised by the device at issue compared to a "substantially equivalent" device already on the market.[18,19] **Figure 1** of the **Supplementary Material** presents a brief overview of these pathways and their typical components. We identified the eight largest medical device categories by advisory committee of assignment. Advisory committees correspond largely to medical specialties (e.g. committees exist for cardiovascular, radiological, and orthopedic devices) and the eight largest committees accounted for over 75%[14,15] of all regulated devices that came to market over this period of time (see **Figure 1** for a summary of how the analysis sample was identified). Modifications to already-marketed devices approved via the "PMA supplement" pathway[20] were excluded.

We used an automated Python script to batch download all associated product summaries and applied *ABBYY FineReader* optical character recognition software (ABBYY, Milpitas, CA) to convert these Portable Document Format (PDF) files into machine-readable text files.

Analysis Sample

We used the US National Institute of Health's National Library of Medicine (NLM) *Medical Text Indexer*[21] (MTI) to identify digital devices as those referencing and/or describing software in their product summaries. The MTI uses natural language processing algorithms that take free text as input and provide medical subject indexing recommendations, based on the MeSH® vocabulary[22] established by the NLM, as output. From a regulatory perspective, products containing software must describe this in their summaries (see above). Indeed, many device summaries contain a short section of the document that is dedicated to describing the product's software (for example, as seen for the Medtronic MiniMed 670G Automated Insulin Delivery System).[23] We used the sample of summaries that were flagged by the MTI as including the medical subject of "software" as our analysis sample of digital devices ("software sample"). In sensitivity analysis, an alternative, keyword-based definition was considered and did not impact findings (**Table 1 and Figure 2 of Supplementary Material**). For each product in the software sample, we recorded each device's FDA decision date (i.e. the year in which the product came to market), its regulatory approval pathway (510(k) or PMA), and the reviewing advisory committee.

Characterization of Cybersecurity Features

The "cybersecurity features" of digital medical devices can take on a number of forms, each of which can address the risks of actions by malevolent parties. Such cybersecurity features may include characterizations or descriptions of a digital product's defensive abilities (e.g. data encryption), an ability to respond to a security breach should it be attempted (e.g. antivirus software), or the ability to detect a breach that has already occurred (e.g. penetration testing).

We searched each of the summaries in the software sample for a pre-specified list of keywords related to cybersecurity content (**Table 2 of Supplementary Material**) and documented use of these keywords (yes/no) in each product summary. These keywords and phrases were selected *a priori* from terminology glossaries from the US National Initiative for Cybersecurity Careers and Studies (NICCS), the FDA's guidance on cybersecurity for medical devices, the US National Institute of Standards and Technology (NIST 4009 / NISTIR 7298) Glossary,[24] and the Manufacturer Disclosure Statement for Medical Device Security (MDS2), a multi-stakeholder devised form designed to give manufacturers a mechanism of disclosing security-related product information to healthcare providers.[25]

Patient and Public Involvement

Patients were not directly involved in the design of this retrospective study of publicly-available regulatory documents. However, popular media accounts of recent cybersecurity concerns in medical devices has brought this previously-obscure topic to the attention of a wide public audience, particularly the millions of patients living with potentially affected devices.[26–28]

Data Analysis

For each year, we identified the software sample and calculated the number and percentage (share) of devices that included cybersecurity content by advisory committee and overall. We compared the percentage of devices with cybersecurity content, as identified by keywords. Using chi-squared tests, we looked at differences between the two major regulatory approval pathways and in earlier versus later years, by comparing the first decade of the period of observation to the final two years.

In order to validate our automated search protocol, we manually reviewed 100 summaries. We selected 50 summaries from the software sample that were identified as containing cybersecurity information, and 50 that were identified as having no such content to confirm text scraping methods. Discrepancies were reviewed by group assent. We further validated our method of identifying devices containing software by electronically scanning all product summaries for the keyword "software" and using these results to assess the sensitivity and specificity of the MTI-defined software sample. (**Supplementary Material**).

All statistical analyses were conducted in STATA version 14.2 (StataCorp LLC, College Station, TX).

Results

A total of 36,430 new devices were identified (**Figure 1**) and of those, 35,794 (98.3%) had product summaries that could be converted to machine-readable text. From this sample, 4,936 new devices (13.79%) were identified by the MTI as including software (9.70% of PMA devices and 13.82% of 510(k) devices. Within the software sample, we found that only 2.13% of devices had product summaries that included cybersecurity content (3.45% of PMA devices and 2.12% of 510(k) devices included cybersecurity content in their summaries, however, differences between PMA and 510(k) devices were not statistically significant [p=0.62]). Manual review confirmed that 100% of summaries included the keyword(s) found by our automated program. Relative to our keyword-based validation exercise, the MTI had a sensitivity of 100% and a specificity of 94.8%, making it a more conservative measure.

Figure 2 presents the share of devices with software over time, while **Figure 3** presents the share of devices in the software sample that included cybersecurity content in their product

summaries over the same period. The overall share of devices including cybersecurity content was higher in recent years, growing from an average of 1.4% in the first decade of our sample to an average of 5.5% in 2015 and 2016, the most recent years included in the sample ($p = 0.0181$). The share of devices including cybersecurity content also varied across regulatory areas from a low of 0% across all years in gastroenterology/urology devices, orthopedic devices, and general/plastic surgery devices, to a high of 22.2% among general hospital devices in 2016 (**Table 1**). **Supplementary Table 2** provides additional detail of the frequencies of individual keywords in the sample.

Discussion

Summary

This study leverages a novel methodology to create an analyzable dataset from public documents describing newly-marketed medical devices. We found that software is an increasingly common component of newly approved or cleared devices, while cybersecurity content in the devices' publicly available product summaries remains rare.

The absence of cybersecurity information for those selecting devices is a concern because it prevents both patients and clinicians from making fully informed decisions about the potential risks associated with the products that they use. This dearth of information may also lead to patients and clinicians to unknowingly adopt products that fail to incorporate appropriate cybersecurity measures. For patients, the risks of software vulnerabilities to safety and privacy can be devastating. A recent study found that hundreds of U.S. medical device recalls have been attributed to software defects—including several recalls of the highest risk to patients.[29] Further, data breaches are already a serious concern for the exposure of sensitive patient data: tens of

millions of records from HIPAA-covered entities have already experienced breaches, with the majority resulting from overt criminal activity, making this risk all the more alarming.[30]

As more and more aspects of healthcare are digitized, the cybersecurity of our healthcare infrastructure—including medical devices—will be increasingly essential to delivering safe and effective care. Recent events such as the emergence of pacemaker vulnerabilities have highlighted both the public health implications of information security[31] and importance of device security.[6] Additionally, the recent security flaws discovered in widely-used computer processors, highlight the fact that new threats continue to emerge[32] and scholars have highlighted medicine as a domain where adversarial attacks may be particularly likely to unfold,[33] with the opportunity for significant clinical impact. Indeed, the NRC has written that "from the standpoint of an individual system or network operator, the only thing worse than being penetrated is being penetrated and not knowing about it."[1] This study is an important first step in understanding the public, transparent reporting of cybersecurity features included in the software embedded in moderate- and high-risk medical devices. Indeed, our characterization of the growing importance of software among regulated devices should encourage policy-makers to buttress FDA's resources accordingly, including support for partnerships with the Department of Homeland Security and other government, academic, and industry partners focused on anticipating and responding to emerging threats to patients and public health.

Limitations

The key limitation of this study is that the information we collected is not a mandatory component of the documents considered. As a result, product summaries may not include all relevant details of a device's design with respect to cybersecurity. While this information may

have been present in other places, such as proprietary applications or the full, confidential FDA dossier, device summaries represent some of the primary documents available for public review, and therefore play an important role in educating stakeholders, such as clinicians, purchasing managers, patients, and administrators of health care systems, about the strength of safety and effectiveness evidence when a new product comes to market. The potential for unobserved information related to cybersecurity content is the key weakness of this study, however the study's key strength is that it is, to our knowledge, the first to take a large-scale approach to characterizing the availability of cybersecurity content among approved medical devices.

Policy Implications

These findings help define the current landscape of medical device software and cybersecurity features, and suggest an opportunity to better inform healthcare professionals, those engaging in device procurement on behalf of hospitals and health care systems, and patients, on the cybersecurity protections embedded in medical devices. In particular, recently-retired FDA Commissioner, Dr. Scott Gottlieb, has publicly acknowledged the importance of the availability of cybersecurity information, noting that "Securing medical devices from cybersecurity threats cannot be achieved by just the FDA alone" and that "every stakeholder – manufacturers, hospitals, health care providers, cybersecurity researchers and gov[ernment] entities [has] a unique role to play in addressing these modern challenges."[34] In the fourth quarter of 2018, in response to the need to "ensure the health care sector is well positioned to proactively respond when cyber vulnerabilities are identified,"[35] the FDA released updated guidance on the content of premarket submissions for the management of cybersecurity in medical devices[10] and the U.S. Department of Health and Human Services similarly recently released voluntary

guidance on cybersecurity practices for healthcare organizations[36]. Ongoing opportunities for the exchange of ideas and best practices among regulators, practitioners, and cybersecurity experts, such as those recently hosted by the FDA on the "management of cybersecurity in medical devices"[37] and collaborations between the security research and medical device communities[38] will be valuable for ensuring public health and a better-informed public and medical community will be crucial to ensuring the safety of medical devices moving forward.

Our findings also support the case for recent proposals by US regulators to include a cybersecurity "bill of materials" in the submission of new medical devices. The proposal calls for "principles and approaches [that] are broadly applicable to all medical devices and are intended to be consistent with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity."[10] Such a standardized approach would represent an important step in addressing the cybersecurity information deficit that we have documented here. Further, many individual hospitals and other purchasers of medical devices currently perform independent information security assessments of medical devices - a slow, resource intensive, and costly process. Standardizing the information security review process and making the results available publicly would bring substantial efficiencies for medical device vendors and healthcare organizations.

Looking Ahead

In an increasingly digitized health care ecosystem, manufacturers will face increasing demands for product safety in the form of cybersecurity protections. Moreover, stakeholders will increasingly seek out information about the safety features of new products. Regulators and manufacturers should collaborate to make the software and cybersecurity content of new

products more easily accessible, and should continue to work together to determine which cybersecurity content should be disclosed and required for regulatory clearance and approval of new products moving forward. It will also be important for future researchers to closely track the availability of cybersecurity content in newly-approved medical devices and to explore whether the publication of such content impacts the product utilization decisions of patients and health care providers.

Figure Legend

Figure 1: Assembly of analysis sample and results

Figure 2: Share of new devices with software ("software sample")

Figure 3: Share of software sample with cybersecurity content

Author Contributions: ADS designed the study in consultation with WJG, ABL, and DBK. ADS collected the data from public sources and performed the primary analysis. All authors had full access to the data and analysis programs for this study and take responsibility for the integrity of the data and the accuracy of the analysis. All authors wrote the manuscript.

Data Sharing Statement: Statistical code and the full dataset are available at https://github.com/arieldora/SternCybersecurityContent

Conflicts of Interest: Dr. Landman is a member of the Abbott Medical Device Cybersecurity Council. Dr. Kramer is supported by the Greenwall Faculty Scholars Program in Bioethics, is a consultant to Circulatory Systems Advisory Panel of the Food and Drug Administration, and has provided consulting to the Baim Institute for Clinical Research for clinical trials of medical devices (unrelated to the study topic). There are no other financial or commercial financial conflicts of interest related to the study topic to report.

Funding: The Harvard Business School Division of Research and Faculty Development supported the data collection for this study. Dr. Stern is supported by the Kauffman Junior

Faculty Fellowship and Dr. Kramer is supported by the Greenwall Faculty Scholars Program in Bioethics.

References

1. National Research Council. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues [Internet]. The National Academies Press; 2014. Available from: https://doi.org/10.17226/18749 [accessed 10 Jul 2018].

2. Burr R. S.754 - 114th Congress (2015-2016): To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. [Internet]. 2015. Available from: https://www.congress.gov/bill/114th-congress/senate-bill/754 [accessed 10 Jul 2018].

3. Blau M. Hospitals brace for security risks that could come with using wearables for patient care [Internet]. STAT. 2017. Available from: https://www.statnews.com/2017/08/04/hospitals-security-risks-wearables/ [accessed 10 Jul 2018].

4. Kuchler H. Medical device makers wake up to cyber security threat. Financial Times [Internet]. 2017 Aug 1; Available from: https://www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691 [accessed 10 Jul 2018].

5. Kramer DB, Fu K. Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. JAMA. 2017 Dec 5;318(21):2077–8.

6. Fox-Brewster T. Medical Devices Hit By Ransomware For The First Time In US Hospitals [Internet]. Forbes. 2017. Available from: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4a76dbe8425c [accessed 10 Jul 2018].

7. IoT guardian for the healthcare industry [Internet]. ZingBox; 2016. Available from: http://www.zingbox.com/wp-content/uploads/2017/02/ZingBox_WP_IoT-Guardian-for-the-Healthcare-Industry.pdf [accessed 10 Jul 2018].

8. Hughes O. WannaCry impact on NHS considerably larger than previously suggested [Internet]. Digital Health. 2017. Available from: https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/ [accessed 10 Jul 2018].

9. Department of Health. Investigation: WannaCry cyber attack and the NHS [Internet]. 2017 Oxtober. Report No.: HC 414. Available from: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [accessed 10 Jul 2018].

10. Food and Drug Administration. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff. Available from: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [accessed 10 Jul 2018].

11. Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff. Available from: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf [accessed 10 Jul 2018].

12. 510(k) Premarket Notification. 2017; Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPMN/pmn.cfm [accessed 10 Jul 2018].

13. Premarket Approval (PMA). 2018; Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPMA/pma.cfm [accessed 10 Jul 2018].

14. Zheng SY, Dhruva SS, Redberg RF. Characteristics of Clinical Studies Used for US Food and Drug Administration Approval of High-Risk Medical Device Supplements. JAMA. 2017 Aug 15;318(7):619–25.

15. Dhruva SS, Bero LA, Redberg RF. Strength of study evidence examined by the FDA in premarket approval of cardiovascular devices. JAMA. 2009 Dec 23;302(24):2679–85.

16. Content of a 510(k). 2017 Oct 31; Available from: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/ucm142651.htm#link_7 [accessed 10 Jul 2018].

17. PMA Application Contents. 2018 Feb 2; Available from: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm050289.htm#ssed [accessed 10 Jul 2018].

18. Kramer DB, Kesselheim AS. User Fees and Beyond — The FDA Safety and Innovation Act of 2012. N Engl J Med. 2012 Oct 4;367(14):1277–9.

19. Kramer DB, Xu S, Kesselheim AS. Regulation of Medical Devices in the United States and European Union. N Engl J Med. 2012 Mar 1;366(9):848–55.

20. Rome BN, Kramer DB, Kesselheim AS. FDA approval of cardiac implantable electronic devices via original and supplement premarket approval pathways, 1979-2012. JAMA. 2014 Jan 22;311(4):385–91.

21. NLM Medical Text Indexer (MTI). 2018; Available from: https://ii.nlm.nih.gov/MTI [accessed 10 Jul 2018].

22. MeSH [Internet]. [cited 2018 Feb 5]. Available from: https://www.ncbi.nlm.nih.gov/mesh [accessed 10 Jul 2018].

23. Summary of Safety and Effectiveness Data (SSED) [Internet]. Available from: https://www.accessdata.fda.gov/cdrh_docs/pdf10/P100034b.pdf [accessed 10 Jul 2018].

24. Kissel R. Glossary of Key Information Security Terms [Internet]. 2013 p. 1–218. Available from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [accessed 10 Jul 2018].

25. Manufacturer Disclosure Statement for Medical Device Security (MDS2). 2017; Available from: http://www.himss.org/resourcelibrary/MDS2 [accessed 10 Jul 2018].

26. How medical devices like pacemakers and insulin pumps can be hacked [Internet]. CBS News. Available from: https://www.cbsnews.com/news/cybersecurity-researchers-show-medical-devices-hacking-vulnerabilities/ [accessed 29 Jan 2019].

27. Gellman L. Insecure Medical Devices Vulnerable to Malicious Hacking [Internet]. Available from: http://nymag.com/intelligencer/2018/08/insecure-medical-devices-vulnerable-to-malicious-hacking.html [accessed 29 Jan 2019].

28. Innes S. "Ethical hackers" are working to warn physicians about cyberattacks [Internet]. 2018. Available from: https://www.azcentral.com/story/news/local/arizona-health/2018/12/27/ethical-hackers-warn-physicians-cyberattacks-christian-dameff-arizona-college-medicine-jeff-tully/2277625002/ [accessed 29 Jan 2019].

29. Ronquillo JG, Zuckerman DM. Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health. Milbank Q. 2017;95(3):535–53.

30. Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. JAMA. 2015 Apr 14;313(14):1471–3.

31. Gordon WJ, Fairhall A, Landman A. Threats to Information Security — Public Health Implications. N Engl J Med. 2017 Aug 24;377(8):707–9.

32. Finlayson SG, Won Chung H, Kohane IS, Beam AL. Adversarial Attacks Against Medical Deep Learning Systems. arXiv [Internet]. 2018 May 21 [cited 2019 Jan 31]; Available from: https://arxiv.org/abs/1804.05296 [accessed 29 Jan 2019].

33. Metz C, Perlroth N. Researchers Discover Two Major Flaws in the World's Computers. The New York Times [Internet]. 2018 Jan 3; Available from: https://www.nytimes.com/2018/01/03/business/computer-flaws.html [accessed 10 Jul 2019].

34. Scott Gottlieb, M.D. on Twitter: "4/4 Securing medical devices from cybersecurity threats cannot be achieved by just the #FDA alone. Every stakeholder—manufacturers, hospitals, health care providers, cybersecurity researchers and govt entities – all have a unique role to play in addressing these modern challenges" [Internet]. 2018. Available from: https://twitter.com/SGottliebFDA/status/1046847875840450560 [accessed 29 Jan 2019].

35. FDA In Brief: FDA proposes updated cybersecurity recommendations to help ensure device manufacturers are adequately addressing evolving cybersecurity threats [Internet]. 2018. Available from: https://www.fda.gov/NewsEvents/Newsroom/FDAInBrief/ucm623624.htm [accessed 29 Jan 2019].

36. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. 36. Available from: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf [accessed 29 Jan 2019].

37. Workshops & Conferences (Medical Devices) > Public Workshop - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices January 29-30, 2019 [Internet]. Available from: https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm623171.htm [accessed 29 Jan 2019].

38. #WeHeartHackers | A collaborative movement between the medical device and security researcher communities. [Internet]. [cited 2019 Jan 31]. Available from: http://wehearthackers.org/ [accessed 29 Jan 2019].

Table 1: Number of devices with machine-readable summaries by FDA/CDRH Advisory Committee and year, share with software and share of software sample with cybersecurity content by Advisory Committee

	FDA/CDRH Advisory Committee							
Year	**Clinical Chemistry** (CH)	**Cardiovascular** (CV)	**Dental** (DE)	**Gastroenterology, Urology** (GU)	**General Hospital** (HO)	**Orthopedic** (OR)	**Radiology** (RA)	**General, Plastic Surgery** (SU)
2002	216	436	318	215	328	403	290	367
2003	192	441	295	233	329	389	329	357
2004	204	395	284	195	270	464	345	319
2005	155	389	245	166	262	480	310	331
2006	197	412	293	142	244	442	338	362
2007	153	358	283	160	257	444	271	319
2008	149	387	279	139	207	477	325	370
2009	130	442	268	155	254	432	290	316
2010	121	390	245	157	280	428	235	312
2011	163	428	258	141	241	542	347	285
2012	155	426	240	166	282	551	344	302
2013	185	428	235	153	202	554	346	301
2014	130	400	225	199	245	583	385	342
2015	108	392	244	179	174	575	340	322
2016	95	368	230	171	204	464	375	354
Totals	2353	6092	3942	2571	3779	7228	4870	4959
Share with software ("software sample")	9.14%	18.99%	4.59%	8.01%	4.97%	1.36%	52.28%	6.96%
Share of software sample with cybersecurity content	7.91%	2.51%	1.66%	0.00%	2.13%	0.00%	2.04%	0.00%

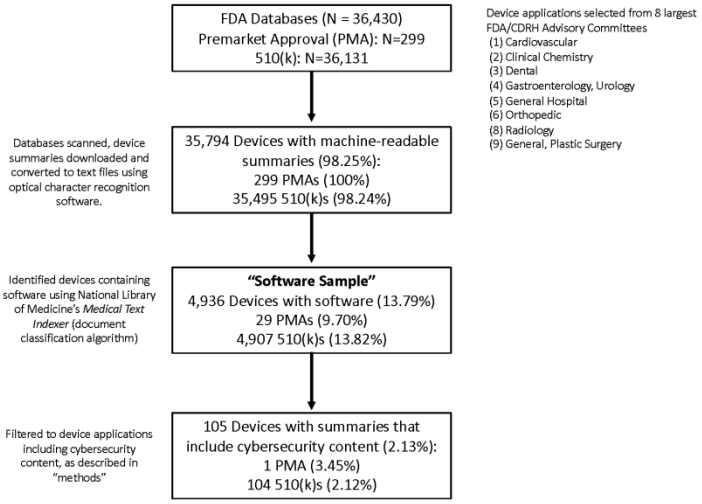


Figure 1: Assembly of analysis sample and results

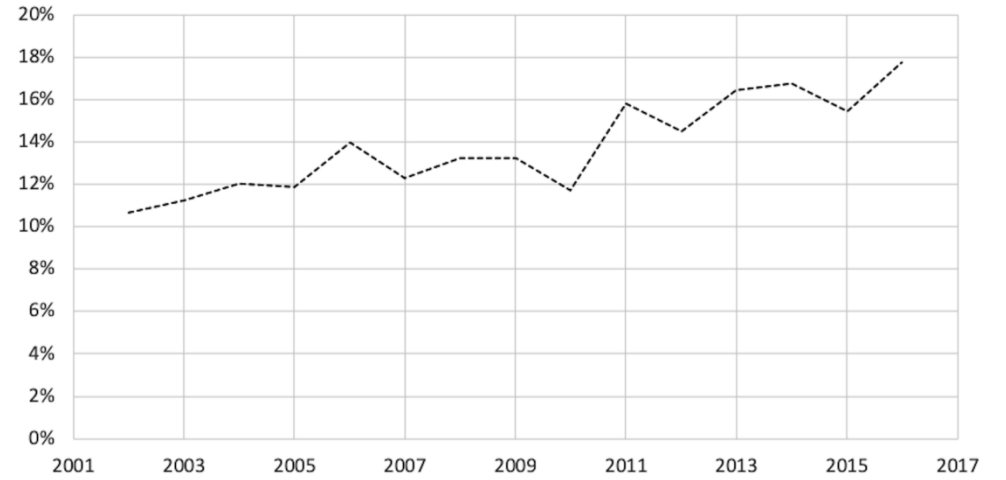


Figure 2: Share of new devices with software ("software sample")

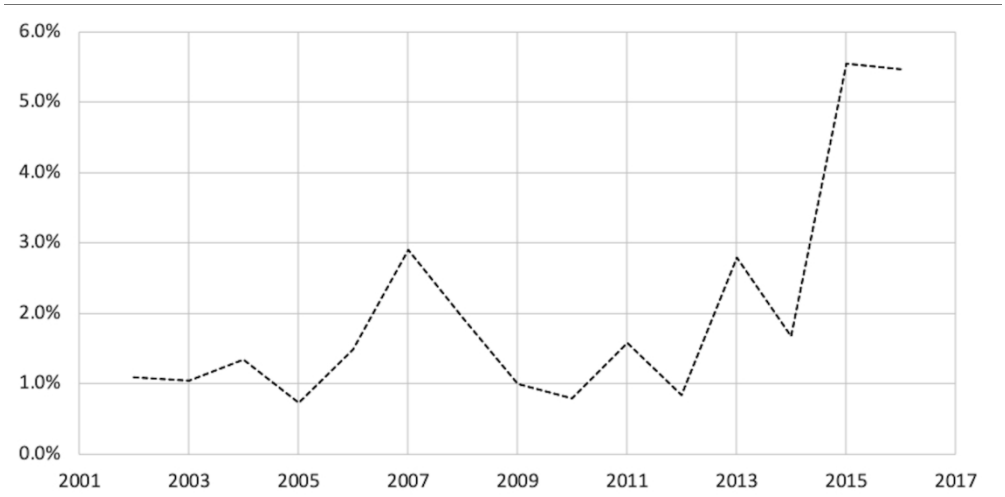


Figure 3: Share of software sample with cybersecurity content

Supplementary Material

I. Processing Using the Medical Text Indexer (MTI)

We sent each of our optical character recognition-processed text files to the MTI and recorded which summaries were classified as being related to software In the MeSH® Tree (ontology). We flagged all products whose summaries were assigned to the "software" MeSH® term, number L01.224.900.

II. Sensitivity Analysis

In sensitivity analyses we considered an alternate method of identifying devices containing software. For this exercise, we electronically scanned each product summary for the keyword "software" and recorded whether the word "software" appeared anywhere within a device's product summary (i.e. at least once in the document).

We expected that the MTI-driven method of identifying the "software sample" would have a high sensitivity but a lower specificity relative to the keyword-based method for the following reason: in order for a text document to be flagged by the MTI's algorithm as being related to the subject of "software" the text document would need describe relevant software content in some detail – i.e. often beyond simply utilizing the keyword "software" at least once.

Indeed, the keyword-based method of identifying software products captured 100% of the products that were identified as including software using the MTI results, but also identified additional products that employ the word "software" in their product summaries at least once (**Supplementary Table**).

Relative to the keyword method, we conclude that the MTI-based method of identifying software products had a 100% sensitivity, but only a 94.8% specificity in our sample. Given the high sensitivity of this method, the MTI-based software sample is the more conservative method for identifying devices with software. However, alternative results using the keyword-based definition are highly similar to those obtained using the MTI-based definition. The total share of the software device sample that includes cybersecurity content is statistically indistinguishable in every year of the sample and visibly similar over time (**Supplementary Table and Supplementary Figure**)

Supplementary Table 1: Comparison of MTI and Keyword-based Methods of Identifying Software over Time

Year	Total Devices	Software sample (MTI defined)	Software sample (keyword defined)	Total devices with cybersecurity content (MTI)	% with cybersecurity content (MTI sample)	Total devices with cybersecurity content (keyword sample)	% with cybersecurity content (keyword)
2002	2573	275	318	3	1.09%	3	0.94%
2003	2565	289	347	3	1.04%	4	1.15%
2004	2476	298	350	4	1.34%	4	1.14%
2005	2338	277	323	2	0.72%	3	0.93%
2006	2430	339	397	5	1.47%	5	1.26%
2007	2245	276	314	8	2.90%	8	2.55%
2008	2333	309	371	6	1.94%	8	2.16%
2009	2287	303	373	3	0.99%	3	0.80%
2010	2168	254	356	2	0.79%	5	1.40%
2011	2405	380	524	6	1.58%	7	1.34%
2012	2466	357	526	3	0.84%	6	1.14%
2013	2404	395	597	11	2.78%	15	2.51%
2014	2509	421	635	7	1.66%	17	2.68%
2015	2334	361	636	20	5.54%	33	5.19%
2016	2261	402	721	22	5.47%	43	5.96%
Totals	35794	4936	6788	105	2.13%	164	2.42%

Supplementary Table 2: List of keywords related to cybersecurity content:

Source	Term	Allowable alternative(s)	Counts
NICCS	access control		17
NICCS	active attack		0
NICCS	air gap		5
NICCS	antispyware software	anti-spyware software, anti-spyware, antispyware	1
NICCS	antivirus software	anti-virus software, anti-virus, antivirus	3
NICCS	asymmetric cryptography		0
NICCS	cipher		0
NICCS	computer network defense		0
NICCS	computer security incident		0
NICCS	cryptanalysis		0
NICCS	cryptographic algorithm		0
NICCS	cryptography		1
NICCS	cyber ecosystem		0
NICCS	cyber exercise		0
NICCS	cyber incident	cyber-incident	0
NICCS	cyber infrastructure	cyber-infrastructure	0
NICCS	cybersecurity	cyber-security	58
NICCS	data breach		0
NICCS	data leakage		0
NICCS	data theft	data-theft	0
NICCS	decrypt		3
NICCS	denial of service	denial-of-service	0
NICCS	designed-in security	designed in security	0
NICCS	digital forensics		0
NICCS	distributed denial of service	distributed denial-of-service, DDOS, D.D.O.S.	0
NICCS	dynamic attack surface		0

NICCS	encrypt		44
NICCS	enterprise risk management		0
NICCS	exploitation analysis		0
NICCS	identity and access management		0
NICCS	information security policy		0
NICCS	information system resilience	Information Systems Security	0
NICCS	Information Systems Security Operations		0
NICCS	intrusion detection		0
NICCS	malicious code		0
NICCS	malware		0
NICCS	NICCS	National Initiative for Cybersecurity Careers and Study	0
NICCS	penetration testing		83
NICCS	phishing		0
NICCS	security incident		0
NICCS	security policy		0
NICCS	spyware	spy-ware	0
NICCS	symmetric cryptography		0
NICCS	symmetric encryption algorithm		0
NICCS	symmetric key		0
NICCS	systems security architecture		0
NICCS	threat assessment		0
FDA Guidance	cybersecurity routine updates and patches	cybersecurity routine updates, cybersecurity routine patches	0
FDA Guidance	cybersecurity signal		0
FDA Guidance	exploit		2
FDA Guidance	Information Sharing Analysis Organizations	ISAO, ISAOs	2
FDA Guidance	NIST	National Institute of Standards and Technology	150
FDA Guidance	NIST Framework	NIST Framework for Improving Critical Infrastructure Cybersecurity	0

Supplementary Figure 1: FDA medical device approval pathways

	Regulatory Pathways for Medical Devices in the United States	
Pathway	510(k) (Premarket Notification)	PMA (Premarket Approval)
Products	Typically moderate-risk ("class II") devices	Typically high-risk ("class III") devices
Requirements	Typically do not necessitate full clinical trials, but require evidence of "substantial equivalence" to a predicate device	Typically require clinical trials to demonstrate a new device's safety and effectiveness
Product develompent time to market	31 months	54 months

Sources:

Maisel WH. Medical device regulation: an introduction for the practicing physician. Annals of internal medicine. 2004 Feb 17;140(4):296-302.

https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k

https://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/premarketsubmissions/premarketapprovalpma

Makower J, Meer A, Denend L. FDA impact on US medical technology innovation: a survey of over 200 medical technology companies. Advanced Medical Technology Association, Washington, DC, available at: http://www. advamed. org/NR/rdonlyres/040E6C33-380B-4F6B-AB58-9AB1C0A7A3CF/0/makowerreportfinal. pdf. 2010 Nov.

Supplementary Figure 2: comparison of main results using alternative method of identifying the software sample