PEER REVIEW HISTORY

ARTICLE DETAILS

TITLE (PROVISIONAL)	Cybersecurity Features of Digital Medical Devices: An Analysis of FDA Product Summaries
AUTHORS	Stern, Ariel; Gordon, William; Landman, Adam; Kramer, Daniel

VERSION 1 - REVIEW

REVIEWER	Diana Zuckerman National Center for Health Research, USA
REVIEW RETURNED	08-Aug-2018

GENERAL COMMENTS	This is an important analysis. I have 2 concerns: 1. On page 9, line 8, the authors say the differences are not statistically significant, but it is not clear what comparison is being made. If they are comparing PMA to 510k, that is very unclear since the PMA and 510k numbers are in parentheses. 2. The Comments don't go beyond the data, but they don't fully reflect the data. The final points made in the Comment section are rather vague and weak. I urge the authors to clarify what kind of cybersecurity information should be included in the summaries and exactly how that information could be useful to health professionals, patients, and providers. This final statement of the manuscript is insufficiently explicit: "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."

REVIEWER	Laurie Pycroft University of Oxford, United Kingdom I have received an honorarium from Kaspersky Lab for consulting work as part of a medical device cybersecurity research project.
REVIEW RETURNED	11-Dec-2018

GENERAL COMMENTS	Overall, this study is a useful and elegant contribution to the rapidly emerging discussion surrounding cybersecurity in medical devices. The application of the MTI to FDA product summaries is a novel method of quantitatively assessing the state of the marketplace. Data has been subjected to appropriate validation and analysis. Their results provide compelling evidence to bolster

	the widespread view within the field that, though manufacturers and regulators are gradually taking cybersecurity more seriously, there is still much to be done before medical devices are acceptably secure. I have two areas of criticism, though both are quite minor. First, I would like to see the results expanded to cover 2017 and, ideally, 2018. Medical device cybersecurity is a swiftly evolving field and I would be interested to see if the increased rate of academic publications in the last few years has preceded a substantial increase in the prominence that manufacturers are placing on security in their FDA filings. That said, if updating the study to cover these years would be prohibitively difficult, I do not think that failure to do so should prevent publication of this paper - it is still of substantial utility on its own and expansion of the results would be worth addressing in future publications. Second, I note some minor issues with the references. Several of the references that include web links do not show the date they were cited and citation 9 misspells "October". I also think that, given the non-specialist nature of the journal, it would be helpful to add one or two more citations of papers that provide a general introduction to medical device cybersecurity for the benefit of interested parties who are not as familiar with the field. Kramer & Fu (2017) is a useful paper in this regard, but adding more such citations would improve the paper's accessibility without necessitating expansion of the text with information that is superfluous to specialists in the field. Other than these small concerns, I think that this paper is an excellent contribution and should certainly be published in BMJ Open.

VERSION 1 – AUTHOR RESPONSE

Reviewer: 1

This is an important analysis. I have 2 concerns:

1. On page 9, line 8, the authors say the differences are not statistically significant, but it is not clear what comparison is being made. If they are comparing PMA to 510k, that is very unclear since the PMA and 510k numbers are in parentheses.

- Thank you for pointing this out. The text in question has been clarified.

2. The Comments don't go beyond the data, but they don't fully reflect the data. The final points made in the Comment section are rather vague and weak. I urge the authors to clarify what kind of cybersecurity information should be included in the summaries and exactly how that information could be useful to health professionals, patients, and providers. This final statement of the manuscript is insufficiently explicit: "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."

- Thank you for these suggestions and comments, which were also echoed in the editor's feedback. We have made a number of substantive updates to the discussion section (formerly the "comments" section) to reflect this feedback and we believe that the updated manuscript represents a more robust, policy-relevant discussion of our study's implications.

***

Reviewer: 2

Overall, this study is a useful and elegant contribution to the rapidly emerging discussion surrounding cybersecurity in medical devices. The application of the MTI to FDA product summaries is a novel method of quantitatively assessing the state of the marketplace. Data has been subjected to appropriate validation and analysis. Their results provide compelling evidence to bolster the widespread view within the field that, though manufacturers and regulators are gradually taking cybersecurity more seriously, there is still much to be done before medical devices are acceptably secure.

I have two areas of criticism, though both are quite minor. First, I would like to see the results expanded to cover 2017 and, ideally, 2018. Medical device cybersecurity is a swiftly evolving field and I would be interested to see if the increased rate of academic publications in the last few years has preceded a substantial increase in the prominence that manufacturers are placing on security in their FDA filings. That said, if updating the study to cover these years would be prohibitively difficult, I do not think that failure to do so should prevent publication of this paper - it is still of substantial utility on its own and expansion of the results would be worth addressing in future publications.

- Thank you for this suggestion. Because we began this project in late 2017, we had ended our data collection with 2016, which represented the last full calendar year for which we could collect complete product data. Given the timeline of manuscript review, over a year has passed since our initial data collection and we recognize that more data would be useful. While we do not currently have the resources to update our analysis sample to reflect additional years of data, we look forward to doing so in future work.

Second, I note some minor issues with the references. Several of the references that include web links do not show the date they were cited and citation 9 misspells "October". I also think that, given the non-specialist nature of the journal, it would be helpful to add one or two more citations of papers that provide a general introduction to medical device cybersecurity for the benefit of interested parties who are not as familiar with the field. Kramer & Fu (2017) is a useful paper in this regard, but adding more such citations would improve the paper's accessibility without necessitating expansion of the text with information that is superfluous to specialists in the field.

- Thank you for your attention to the references and suggestions for additional citations. We have standardized the formatting of references and added citation dates for web links. We have also added additional references to further ground our study in the existing literature, including the Kramer and Fu reference.

VERSION 2 – REVIEW

REVIEWER	Diana Zuckerman National Center for Health Research USA
REVIEW RETURNED	08-Apr-2019

GENERAL COMMENTS	Page 4, Introduction – Paragraphs 2-3 The authors discuss cybersecurity in the context of different health information technologies and medical devices. The risks of software vulnerabilities to patient safety and privacy should also be emphasized and supported with references from the literature. Some suggested examples: --“Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health” Milbank Q. 2017 Sep;95(3):535-553. https://www.ncbi.nlm.nih.gov/pubmed/28895231 --"Review of Reported Clinical Information System Adverse Events in US Food and Drug Administration Databases”. Appl Clin Inform. 2011;2(1):63-74. https://www.ncbi.nlm.nih.gov/pubmed/21938265 -- "Data Breaches of Protected Health Information in the United States" JAMA. 2015 Apr 14;313(14):1471-3. https://www.ncbi.nlm.nih.gov/pubmed/25871675 -- "Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health" Milbank Quarterly 2017 September 95(3);535-553. https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-0009.12278 Page 6, Line 42 For the informatics pipeline that was developed to convert raw data into machine readable form, additional details about the “automated script” (e.g. programming language(s), etc.) would be useful. Page 8, Line 51-52 Current definition of “earlier versus later years” for chi-square test is unclear. Author should provide a more explicit definition in this section of the Methods. Page 10, Discussion The authors highlight that the cybersecurity content in publicly available device summaries is currently very rare. Authors should

	describe how this potentially affects patient safety and the implications at the individual and population levels. Page 27, Line 14-17 (Supplementary Figure 1) Description of 510(k) is incorrect. It states: “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” On the contrary, as noted by the Institute of Medicine in their 2011 report, the 510(k) process rarely requires any clinical trials (full or otherwise) and the predicate device is also not required to be proven either safe or effective.

REVIEWER	Laurie Pycroft University of Oxford, UK
REVIEW RETURNED	05-Mar-2019

GENERAL COMMENTS	I'm pleased to see the changes that the authors have added since the last version of the document, particularly the improved discussion of the study's limitations. I recommend that the paper be published.

VERSION 2 – AUTHOR RESPONSE

Reviewer: 1

Reviewer Name: Diana Zuckerman

Institution and Country: National Center for Health Research, USA

Please state any competing interests or state ‘None declared’: None declared

Please leave your comments for the authors below

Page 4, Introduction – Paragraphs 2-3

The authors discuss cybersecurity in the context of different health information technologies and medical devices. The risks of software vulnerabilities to patient safety and privacy should also be emphasized and supported with references from the literature. Some suggested examples:

--“Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health” Milbank Q. 2017 Sep;95(3):535-553.

https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ncbi.nlm.nih.gov%2Fpubmed%2F28895231&data=02%7C01%7Castern%40hbs.edu%7Cb99109eefbe4420b8e2308d6d47f8abe%7C09fd564ebf4243218f2db8e482f8635c%7C0%7C0%7C636930041584415906&sdata=HYE%2FjST1oeuwtc3XyglLp%2BmlIDLEE7DNc0c%2FXbWo4jQ%3D&reserved=0

--"Review of Reported Clinical Information System Adverse Events in US Food and Drug Administration Databases". Appl Clin Inform. 2011;2(1):63-74. https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ncbi.nlm.nih.gov%2Fpubmed%2F21938265&data=02%7C01%7Castern%40hbs.edu%7Cb99109eefbe4420b8e2308d6d47f8abe%7C09fd564ebf4243218f2db8e482f8635c%7C0%7C0%7C636930041584425910&sdata=ZiixJx8YgM%2BlEBhq66yFoJUueEfFMqoHIUtsEE1wcHs%3D&reserved=0

-- "Data Breaches of Protected Health Information in the United States" JAMA. 2015 Apr 14;313(14):1471-3. https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ncbi.nlm.nih.gov%2Fpubmed%2F25871675&data=02%7C01%7Castern%40hbs.edu%7Cb99109eefbe4420b8e2308d6d47f8abe%7C09fd564ebf4243218f2db8e482f8635c%7C0%7C0%7C636930041584425910&sdata=6f1aodCSwFkrTZVNG5yJd6u8FWiStdAf0REHYVxtspk%3D&reserved=0

-- "Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health" Milbank Quarterly 2017 September 95(3);535-553. https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fonlinelibrary.wiley.com%2Fdoi%2Fabs%2F10.1111%2F1468-0009.12278&data=02%7C01%7Castern%40hbs.edu%7Cb99109eefbe4420b8e2308d6d47f8abe%7C09fd564ebf4243218f2db8e482f8635c%7C0%7C0%7C636930041584425910&sdata=KRY2Y8MPQSUVr1gePoMnK8p5AeuFPMZr%2B8Cy%2BlzlWhs%3D&reserved=0

Thank you for this helpful suggestion and for providing fitting references. We have incorporated this recommendation into a new paragraph on pages 10 and 11 of the manuscript.

Page 6, Line 42

For the informatics pipeline that was developed to convert raw data into machine readable form, additional details about the "automated script" (e.g. programming language(s), etc.) would be useful.

We have updated this sentence to clarify that Python was the programming language used for this script.

Page 8, Line 51-52

Current definition of “earlier versus later years” for chi-square test is unclear. Author should provide a more explicit definition in this section of the Methods.

This is now clarified on page 8, in addition to the same detail that was already presented in the “Results” section; our apologies for the confusion.

Page 10, Discussion

The authors highlight that the cybersecurity content in publicly available device summaries is currently very rare. Authors should describe how this potentially affects patient safety and the implications at the individual and population levels.

We have added a paragraph in the Discussion (currently on pages 10-11) that addresses this comment as well as the first comment above.

Page 27, Line 14-17 (Supplementary Figure 1)

Description of 510(k) is incorrect. It states: “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”

On the contrary, as noted by the Institute of Medicine in their 2011 report, the 510(k) process rarely requires any clinical trials (full or otherwise) and the predicate device is also not required to be proven either safe or effective.

We have updated the text in this Figure to remove the phrase “, which has been shown to be safe and effective.”