Viewpoint

The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint

Beau Woods[1,2,3*], BS; Andrea Coravos[1,4,5,6*], MBA; Joshua David Corman[1,3,7,8*], BA

[1]I Am The Cavalry, Washington, DC, United States
[2]Biohacking Village, New York, NY, United States
[3]Atlantic Council, Washington, DC, United States
[4]Elektra Labs, Boston, MA, United States
[5]Harvard-MIT Center for Regulatory Science, Harvard University, Boston, MA, United States
[6]Digital Medicine (DiMe) Society, New York, NY, United States
[7]Heinz College of Information Systems and Public Policy, Carnegie Mellon University, Pittsburgh, PA, United States
[8]PTC, Needham, MA, United States
[*]all authors contributed equally

Corresponding Author:
Andrea Coravos, MBA
Elektra Labs
Harvard Innovation Labs
125 Western Ave
Boston, MA, 02163
United States
Phone: 1 9788421240
Email: andrea@elektralabs.com

Abstract

Prior to graduating from medical school, soon-to-be physicians take the Hippocratic Oath, a symbolic declaration to provide care in the best interest of patients. As the medical community increasingly deploys connected devices to deliver patient care, a critical question emerges: should the manufacturers and adopters of these connected technologies be governed by the symbolic spirit of the Hippocratic Oath? In 2016, I Am The Cavalry, a grassroots initiative from the cybersecurity research community, published the first Hippocratic Oath for Connected Medical Devices (HOCMD), containing 5 principles. Over the past three years, the HOCMD has gained broad support and influenced regulatory policy. We introduce 5 case studies of the HOCMD in practice, illustrating how the 5 principles can lead to a safer and more effective adoption of connected medical technologies.

(J Med Internet Res 2019;21(3):e12568) doi: 10.2196/12568

KEYWORDS

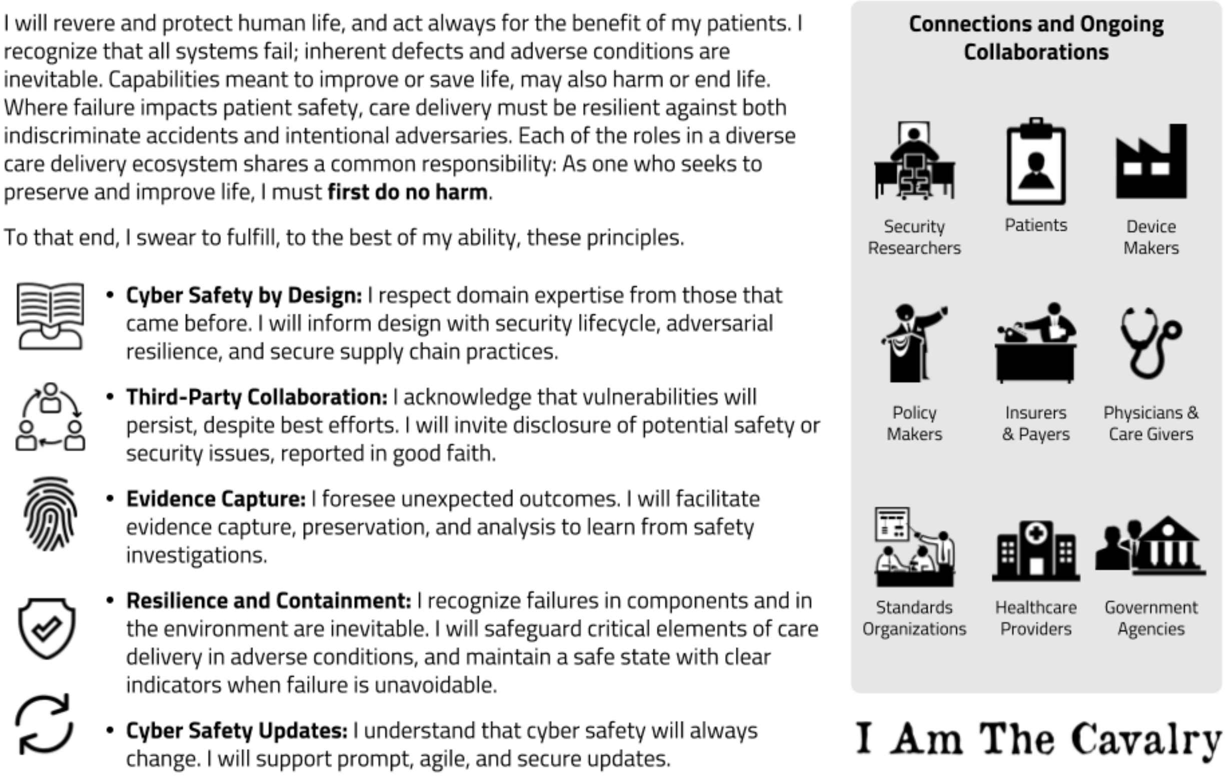
ethics; cybersecurity; information technology; delivery of health care; connected devices

Introduction

Prior to graduating from medical school, soon-to-be physicians take the Hippocratic Oath [1], a symbolic declaration to provide care in the best interest of patients. As the medical community increasingly deploys connected devices to deliver patient care, a critical question emerges: should the manufacturers and adopters of these connected technologies be governed by the symbolic spirit of the Hippocratic Oath?

Five years ago, Joshua David Corman and Nicholas Percoco founded *I Am The Cavalry*, a grassroots initiative from the cybersecurity research community. Its mission is “to ensure technologies with the potential to impact public safety and human life are worthy of our trust” [2]. In 2016, along with a diverse stakeholder group across the health care ecosystem, including payers, providers, patients, policy makers, and physicians, I Am The Cavalry drafted the first version of a Hippocratic Oath for Connected Medical Devices (HOCMD) (see Figure 1) and published an open letter on its website [3]. Similar to graduating medical students who pledge to protect the patient and hospital systems who pledge to protect patients’ data and information, the HOCMD outlines five guiding ethical principles for manufacturers, organizations, and individuals delivering care through connected medical devices.

Figure 1. Hippocratic Oath for Connected Medical Devices (HOCMD).



I will revere and protect human life, and act always for the benefit of my patients. I recognize that all systems fail; inherent defects and adverse conditions are inevitable. Capabilities meant to improve or save life, may also harm or end life. Where failure impacts patient safety, care delivery must be resilient against both indiscriminate accidents and intentional adversaries. Each of the roles in a diverse care delivery ecosystem shares a common responsibility: As one who seeks to preserve and improve life, I must **first do no harm**.

To that end, I swear to fulfill, to the best of my ability, these principles.

- **Cyber Safety by Design:** I respect domain expertise from those that came before. I will inform design with security lifecycle, adversarial resilience, and secure supply chain practices.
- **Third-Party Collaboration:** I acknowledge that vulnerabilities will persist, despite best efforts. I will invite disclosure of potential safety or security issues, reported in good faith.
- **Evidence Capture:** I foresee unexpected outcomes. I will facilitate evidence capture, preservation, and analysis to learn from safety investigations.
- **Resilience and Containment:** I recognize failures in components and in the environment are inevitable. I will safeguard critical elements of care delivery in adverse conditions, and maintain a safe state with clear indicators when failure is unavoidable.
- **Cyber Safety Updates:** I understand that cyber safety will always change. I will support prompt, agile, and secure updates.

Adopting these principles not only builds trust in the connected product for patients, clinicians, hospitals, and regulators, but also serves a business function. Similar to a drug that is pulled off the market because of unintended side effects, connected products with security vulnerabilities can sharply impact a company's share price and valuation. For medical device investors who want to avoid security issues in their portfolio companies, these principles enable them to evaluate a connected medical product's risk profile, safety, and effectiveness.

Although all systems eventually fail, not all failures have to cause harm. Organizations that follow these five principles tend to build safer products with fewer malfunctions and deliver better care to patients. To illustrate the principles, we have outlined five case studies based on true events; we have blinded some examples at the request of the parties involved.

Five Case Studies based on the 5 Oath Principles

Oath Principle #1: Cyber Safety by Design

Riley, a hospital procurement analyst, reviews several medical devices, struggling to distinguish security features between similar products and the potential impact on cost and risk to her organization. Riley and her peers often rely on sales literature and expensive internal testing to understand how to buy the best devices to fit their clinical environments. Products with better documentation make her job easier and increase the organization's confidence that the devices can be deployed and used safely and effectively, without undue cost or risk.

Riley prefers to procure devices from manufacturers who follow practices laid out in *cyber safety by design*, because she can more easily anticipate and avoid product failures. For example, preferred devices would have instructions for safe and secure implementation, design assumptions, a *software bill of materials* (SBOM), and other documentation outlining how cybersecurity is designed into the product's lifecycle. Health care organizations like the Mayo Clinic have started requiring manufacturers to disclose more information about their security capabilities [4]. These requirements are being widely adopted by manufacturers like Philips, Siemens, and Becton Dickinson, and are becoming standard practice through industry-led initiatives like the Manufacturer Disclosure Statement for Medical Device Security (MDS2) disclosures [5].

This past year, the US Food and Drug Administration (FDA) incorporated the *cyber safety by design* principles in their Medical Device Safety Action Plan [6] and updated Premarket Guidance [7], which proposes requiring an SBOM or *cybersecurity bill of materials* (CBOM), in which manufacturers have to clearly communicate choices and capabilities that impact cyber safety and other practices from this first principle.

Oath Principle #2: Third-Party Collaboration

In early 2017, Jay Radcliffe, a researcher with the security firm Rapid7, discovered a flaw in how the Johnson & Johnson Animas insulin pumps handle commands from the unit's remote control. Exploiting the flaw could potentially lead to unauthorized access to the pump through its unencrypted radio frequency communication system.

Undisclosed flaws represent potential harm to patients through accidents or adverse events. While it may seem inconceivable, many manufacturers have threatened security researchers with legal repercussions [8] for identifying these kinds of issues. Although immediate public disclosure often catalyzes a prompt fix, releasing the disclosure often starts a footrace between defenders and adversaries that may put patients at greater risk. Jay had a difficult decision to make: should he disclose the vulnerability and, if so, how?

Thankfully, Johnson & Johnson had recently drafted a coordinated disclosure policy that invited third-party collaboration. After investigation, the issue was considered to be a low safety risk due to existing mitigations. Jay and Johnson & Johnson codeveloped an effective approach to addressing the issue, communicated with patients and physicians, kept the FDA and other organizations informed, and improved internal processes. This was a win for all involved and decreased potential harm to patients.

Many throughout the health care ecosystem, including regulators like the FDA, are voicing their support for coordinated vulnerability disclosure. The FDA recently outlined this principle in their guidance for Post-Market Management of Cybersecurity in Medical Devices [9] and published a collaborative report with the Medical Device Innovation Consortium (MDIC) that advances the concept of coordinated disclosure [10]. Perhaps untraditionally, the FDA has also started to participate at hacker conferences like DEF CON [11] to encourage greater collaboration when surfacing vulnerabilities.

As of this writing, nearly 20 companies have published programs [12] to receive and handle reports of security vulnerabilities. Programs based around standards (ie, ISO 29147, ISO 30111, and National Telecommunications and Information Administration [NTIA] Early Stage Template [13]) frequently leverage existing mechanisms internally that are well-tested and focus on incentives, aligning researchers and device makers toward safer products.

Oath Principle #3: Evidence Capture

Two years ago, a hospital sent a life-critical device to the manufacturer for investigation, suspecting that it was tampered with by a physician who was being sued for malpractice. After conducting a review, the manufacturer discovered that evidence of patient care had been wiped from the device, but it was unclear who did this, when, or why. The connected device lacked forensically sound evidence-capture tools.

When doctors are not sure why an adverse event happened, they perform tests or, in the case of death, an autopsy. When medical devices are involved, evidence from the device can and should support postmortem investigations as part of that autopsy. For this reason, the third principle of the Oath, *evidence capture*, alerts manufacturers to the need for built-in evidence-capture capabilities and tamper-evident logging to protect patients.

For instance, a secure system could store a fixed record of safety- and security-related data, such as software integrity checks and activity logs. This information could then be reviewed by analysts at the health care organization or the manufacturer to support investigations into malicious tampering, accidental harm, or cybersecurity issues. In addition, this capability lays the foundation for future capabilities that allow for more prompt and agile responses.

The FDA's recent draft premarket guidance [7] calls for a forensically sound evidence-capture capability, despite relatively little interest from industry and regulatory bodies. This capability would be invaluable; most devices currently lack activity logs and other integrity checks, indicating that it is possible that there have been adverse events related to device malfunction of which manufacturers are unaware. The FDA's updated guidance will likely incentivize more device makers to include this capability in their products.

Oath Principle #4: Resilience and Containment

In 2017, several German journalists sat in a room learning how to hack medical devices at a press event held by Dräger. First, they learned how to use tools to penetrate a basic installation of Windows XP, an operating system that had been unsupported for three years. After gaining complete control of the ventilators, the journalists tried similar techniques against a version of Windows XP that Dräger uses in some of its current products. None of the journalists, nor the subsequent professional penetration testers, were able to hack the device over the network. The company had hardened the system by disabling nonessential functions, encrypting data in transit, and isolating the network-connected elements from those that deliver patient care.

Medical devices are increasingly connected to the rest of the hospital and to the Internet. A traditional stethoscope or ultrasound are not connected to each other, let alone exposed to technically savvy adversaries thousands of miles away. Practices in the *resilience and containment* principle can contain the reach of adversaries by reducing risk from cascading cybersecurity failures, making failures evident, and ensuring devices default to a safe mode when they must fail.

Building on the *resilience and containment* principle, the FDA's premarket guidance outlines best practices, such as improving device isolation using firewalls, reducing elective exposure by disabling network-connected components, and protecting patient record integrity by encrypting data while in transit and on the device. The FDA has also issued two safety notifications related to failure to segregate safety-critical from noncritical components of Hospira infusion pumps [14,15].

Oath Principle #5: Cyber Safety Updates

In 2016, a vulnerability was discovered in St. Jude Medical's pacemakers, implantable cardioverter defibrillators, and bedside monitors. The chances that an adversary would exploit this vulnerability to cause harm seemed low, but the attack could be carried out stealthily, triggering heart conditions in patients. An estimated 465,000 patients would be at risk before the manufacturer could build replacements and doctors could implant them [16].

Fortunately, St. Jude Medical had a better way to address the issue. A series of three software updates greatly reduced cost, increased adoption, hastened correction timelines, and minimized side effects compared to extreme solutions, such as replacing the device through explantation. A study showed that 25% of patients had the software update applied at their next clinic visit, with no pacing failures observed [17].

It should be common practice to update software routinely. The FDA has repeatedly stated that manufacturers are responsible for delivering security updates, which are considered routine and therefore not often subject to additional reviews. However, security and promptness of these updates still lag for most device makers and communication is difficult with many stakeholders involved with each device.

Accelerating Adoption of the Hippocratic Oath for Connected Medical Devices

While most doctors practicing in the United States take the Hippocratic Oath before going into clinical practice, developers of software-connected devices traditionally do not share a similar gatekeeper. As of today, individuals and organizations can publicly commit to the HOCMD via the I Am The Cavalry website [3]. Though this lacks the resonance of repeating the Oath aloud at a hard-earned graduation, the digital pledge carries its own gravitas. Digital statements are accessible and searchable. An online pledge holds leadership, scientists, and engineers accountable for their work by the public and signals an unwavering faith in the quality of the products they have created. The Oath can also be taken by organizations, like hospital systems, who pledge to act not only in the best interest of the corporal patient, but also in the best interest of the patient's information—the patient's *digital specimen*.

Oaths can serve two important purposes: first, to establish a set of standards and second, to remind an oath-taking community of their promised commitments. Although oaths have a storied history, evidence does not necessarily suggest that taking an oath leads to better behavior in practice even within medical professions [18]. Thus, as the HOCMD matures, its principles may be deployed more effectively in other formats. For instance, a checklist may be a more effective format than an oath for putting the principles into routine practice [19]. Atul Gawande popularized practical checklists in health care when he published The Checklist Manifesto, a short book on how not to make big mistakes, and outlined how a checklist format can increase efficiency, consistency, and safety [20].

The HOCMD's influence on regulatory policy is another example of its principles moving from theory to practice. Although the FDA draft guidance for Management of Cybersecurity in Medical Devices, published in October 2018, does not call out the Oath by name, it references four Oath principles in its premarket guidance [7] and references the fifth in its postmarket guidance [9]. FDA officials have shared in speeches [11] and tweets [21] their learnings from the security and hacker communities as they draft modern policies to bring safe, connected, medical products to market.

We envision a world where all medical device manufacturers stand proudly behind their work by publicly committing to upholding these principles of cyber safety; we also envision a world where patients, hospitals, doctors, insurers, and regulators strongly favor more secure medical devices built by manufacturers who align with the Oath. As software-driven connected products drive more care delivery, we hope that those who manufacture and adopt life-critical products will commit to carrying similar values as the physicians who have attended to patients for centuries.

Acknowledgments

For suggesting compelling examples of Oath principles and reviews of the case studies, we gratefully acknowledge Jay Radcliffe, MS; Chris Tyberg; Hannes Molsen; Colin Morgan; Ginny Fahs; Ana Sofia Warner, MD; Stacey Higginbotham; Adam Conner-Simons; Janine Medina, MS; and the Biohacking Village at DEF CON. AC acknowledges support from Harvard-MIT Center for Regulatory Science. We also want to recognize the I Am The Cavalry working group, who drafted the original Hippocratic Oath for Connected Medical Devices.

Conflicts of Interest

The authors are members of I Am The Cavalry, the grassroots organization that drafted the Hippocratic Oath for Connected Medical Devices. I Am The Cavalry is an entirely volunteer effort without legal incorporation status.

References

1. Tyson P. PBS. 2001 Mar 27. The Hippocratic Oath today URL: https://www.pbs.org/wgbh/nova/article/hippocratic-oath-today/ [accessed 2018-10-22] [WebCite Cache ID 73Lh06EQQ]
2. I Am The Cavalry. URL: https://www.iamthecavalry.org/ [accessed 2019-01-02] [WebCite Cache ID 757vwSlS2]
3. I Am The Cavalry. Hippocratic Oath for Connected Medical Devices URL: https://www.iamthecavalry.org/domains/medical/oath/ [accessed 2018-10-20] [WebCite Cache ID 73Ij9CNM9]
4. Medical and Research Device Risk Assessment Vendor Packet Instructions. Rochester, MN: Mayo Clinic; 2018. URL: https://www.mayoclinic.org/documents/medical-device-vendor-instructions/doc-20389647 [accessed 2018-10-20] [WebCite Cache ID 73IjdfDIl]

5. National Electrical Manufacturers Association (NEMA). 2013 Oct 07. Manufacturer disclosure statement for medical device security URL: https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx [accessed 2018-10-21] [WebCite Cache ID 73KmoQ4Ao]
6. Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health. Silver Spring, MD: US Food and Drug Administration; 2018. URL: https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf [accessed 2018-10-21] [WebCite Cache ID 73KvY8HRa]
7. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD: Center for Devices and Radiological Health, US Food and Drug Administration; 2018 Oct 18. URL: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf [accessed 2018-10-21] [WebCite Cache ID 73WNSLF4s]
8. Whittaker Z. ZDNet. 2018 Feb 19. Lawsuits threaten infosec research — just when we need it most URL: https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/ [accessed 2018-10-21] [WebCite Cache ID 73KwFicUC]
9. Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD: Center for Devices and Radiological Health, US Food and Drug Administration; 2016 Dec 28. URL: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf [accessed 2018-10-21] [WebCite Cache ID 73KwPnl1c]
10. Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure. Arlington, VA: Medical Device Innovation Consortium (MDIC); 2018. URL: http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf [accessed 2018-10-21] [WebCite Cache ID 73KwojnAP]
11. Gottlieb S. US Food and Drug Administration. 2018 Oct 01. Statement from FDA Commissioner Scott Gottlieb, MD on FDA’s efforts to strengthen the agency’s medical device cybersecurity program as part of its mission to protect patients URL: https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/UCM622074.htm [accessed 2018-10-22] [WebCite Cache ID 73LhhBvmf]
12. I Am The Cavalry. Vulnerability disclosure programs URL: https://www.iamthecavalry.org/resources/disclosure-programs/ [accessed 2018-10-21] [WebCite Cache ID 73KxNazAS]
13. "Early Stage" Coordinated Vulnerability Disclosure Template. Version 1.1. Washington, DC: NTIA Safety Working Group; 2016 Dec 15. URL: https://webcache.googleusercontent.com/search?q=cache:mbJ9mUcs-_IJ:https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf+&cd=1&hl=en&ct=clnk&gl=us [accessed 2019-02-25] [WebCite Cache ID 76SW6QYuN]
14. Finkle J. Reuters. 2015 Jul 31. FDA warns of security flaw in Hospira infusion pumps URL: https://www.reuters.com/article/us-hospira-fda-cybersecurity/fda-warns-of-security-flaw-in-hospira-infusion-pumps-idUSKCN0Q52GJ20150731 [accessed 2018-10-22] [WebCite Cache ID 73Lij10Tw]
15. The Security Ledger. 2015 May 14. FDA safety advisory warns of cyber risk of drug pumps URL: https://securityledger.com/2015/05/fda-safety-advisory-warns-of-cyber-risk-of-drug-pumps/ [accessed 2018-10-22] [WebCite Cache ID 73Lj58ZRQ]
16. US Food and Drug Administration. 2017 Aug 29. Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers: FDA safety communication URL: https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm573669.htm [accessed 2019-02-19] [WebCite Cache ID 76J0ovzrJ]
17. Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE. Factors influencing the decision to proceed to firmware upgrades to implanted pacemakers for cybersecurity risk mitigation. Circulation 2018 Sep 18;138(12):1274-1276. [doi: 10.1161/CIRCULATIONAHA.118.034781] [Medline: 29748188]
18. Sierles F, Kushner B, Krause P. A controlled experiment with a medical student honor system. J Med Educ 1988 Sep;63(9):705-712. [Medline: 3418674]
19. Loukides M, Mason H, Patil DJ. Ethics and Data Science. Sebastopol, CA: O’Reilly Media, Inc; Jul 2018.
20. Gawande A. The Checklist Manifesto: How to Get Things Right. New York, NY: Metropolitan Books; 2010.
21. Gottlieb S. Twitter. 2018 Oct 07. Twitter post URL: https://twitter.com/SGottliebFDA/status/1048987791596642310 [accessed 2019-02-19] [WebCite Cache ID 76J0PZkHp]

Abbreviations

CBOM: cybersecurity bill of materials
FDA: US Food and Drug Administration
HOCMD: Hippocratic Oath for Connected Medical Devices
MDIC: Medical Device Innovation Consortium
MDS2: Manufacturer Disclosure Statement for Medical Device Security
NTIA: National Telecommunications and Information Administration
SBOM: software bill of materials

Edited by G Eysenbach, E Perakslis; submitted 01.11.18; peer-reviewed by K McDonald, P Lynch, J Suleder; comments to author 28.11.18; revised version received 23.01.19; accepted 28.01.19; published 19.03.19

Please cite as:
Woods B, Coravos A, Corman JD
The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint
J Med Internet Res 2019;21(3):e12568
URL: http://www.jmir.org/2019/3/e12568/
doi: 10.2196/12568
PMID: 30888323