Journal of Pain Research

Dovepress
Taylor & Francis Group

Open Access Full Text Article

ORIGINAL RESEARCH

Evaluating Physician Knowledge of Data Privacy and Cybersecurity Risks in Neuromodulation: An Online Cross-Sectional Survey

Everette Martin[1], Erika Petersen[2], Jarna R Shah[3]

[1]College of Medicine, University of Arkansas for Medical Sciences, Little Rock, AR, USA; [2]Department of Neurosurgery, University of Arkansas for Medical Sciences, Little Rock, AR, USA; [3]Department of Anesthesiology, University of Arkansas for Medical Sciences, Little Rock, AR, USA

Correspondence: Everette Martin, University of Arkansas for Medical Sciences, 4301 W Markham St, Little Rock, AR, USA, Email elmartin@uams.edu

Purpose: Data privacy and cybersecurity should both be seriously considered for all devices that interact with our patients. There is little education of patients and clinicians about the cybersecurity and privacy of implanted medical devices, and these considerations are likely not part of informed consent discussions. The FDA has made efforts to remedy this, including releasing suggestions on how best to counsel patients and updating industry cybersecurity considerations, however they are not currently legally binding.

Participants and Methods: In this online survey, we assess the awareness, understanding, and interest of clinicians implanting neuromodulation devices in the topics of cybersecurity and device privacy.

Results: Clinicians were limited in their familiarity and awareness of these topics. The majority of responders do not counsel their patients on device cybersecurity and only sometimes counsel them on data privacy.

Conclusion: Patients and providers may have limited knowledge of data privacy and cybersecurity in implanted medical devices and further education should be undertaken to promote the impact of these issues.

Keywords: data privacy, cybersecurity, neuromodulation, implanted devices

Introduction

The Implantable Medical Device (IMD) market, already valued as a billion-dollar industry, is projected to nearly double within the next decade.[1] Advances in IMDs that allow for wireless communication have enabled healthcare providers new capabilities such as remotely programming devices and monitoring patients.[2] Unfortunately, reliance on software and internet for wireless communication with IMDs allows for vulnerabilities to outside attack.

Hackers have the potential to track and steal health data, and they may even have the ability to compromise the therapeutic effect of the device.[3] The FDA has recognized the importance of device security through published requirements for new device development.[4] Patients with neuromodulation devices represent a unique group of potential targets to hackers because of the data points these devices collect and can transmit and the perceived intimate connection of these devices to patients' nervous systems.

Implanted neuromodulation devices for movement disorders, epilepsy and pain can track and record patient data such as demographic information, activity tracking and physiologic recordings, which can then be downloaded to hospital, office or manufacturer sites for review. These data can be collected and stored indefinitely, allowing for retrospective analysis, however, there are serious concerns about the privacy of data collected from implanted devices.[4,5] Only recently efforts have been made to educate patients and clinicians about the cybersecurity of medical devices, the data collected, and its use and possible misuse.[6,7] Unfortunately, these considerations are rarely part of informed consent discussions. The business relationship between the patient and the manufacturer of their device, the statement of Terms of Service, and discussion of how patients might opt out of data collection vary in how they are communicated to patients and clinicians. This is uncharted territory, and practitioners need guidance on appropriate management of these devices.

Received: 17 December 2024
Accepted: 11 June 2025
Published: 24 June 2025

With the growing interest and volume of implanted medical devices on the market and the larger affected patient population, there is a high level of importance of proper device cybersecurity. Until last year, government agencies did not explicitly dictate requirements for medical device cybersecurity. In March 2023, the FDA released a set of guidelines for manufacturers to follow with the "Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices Under Section 524B of the FD&C Act."[8] Recommendations in the document include disclosing potential vulnerabilities and demonstrating that the device is cyber-secure. It should also be noted, however, that the document is a set of guidelines that "do not establish legally enforceable capabilities" and are relatively vague. While this policy may be a step in the right direction, much more needs to be done to ensure comprehensive legislation that protects patient privacy and security.

Healthcare providers bear the responsibility of educating patients on the privacy and cybersecurity risks involved with IMD's. This includes a thorough discussion of the risks, benefits, and protective measures in place. As the latter are relatively new issues, guidelines have been unclear regarding what physicians should touch upon.[9] No guidelines have yet been established for clinicians who wish to communicate issues specific to implantable neuromodulation devices. In order to create practical guidelines, research should be done to learn what physicians who implant these devices understand about data privacy and cybersecurity in neuromodulation systems. Thus, the purpose of this study is to investigate provider knowledge of neuromodulation device cybersecurity and data privacy using online social media dissemination, in order to gauge the level of awareness, familiarity, and emphasis that physicians place on these issues.

Methods

Study Design

This survey study was approved by the University of Arkansas for Medical Sciences Institutional Review Board. Online surveys were sent via social media platforms and society listservs to characterize knowledge of cybersecurity in neuromodulation devices. The survey window extended from September to October 2022. Surveys were sent out via selected social media platforms (LinkedIn and X, formerly Twitter), with weekly posts. In addition, one large Email database of registered physician implanters via the international pain society was utilized one time to capture participants. The survey was closed after seven days. Participants were administered an online survey consisting of twelve questions. The survey consisted of polar questions (yes/no) and Likert scale based questions to allow rating of knowledge from "not very comfortable" to "very comfortable". The survey also included two optional open response questions. A total of 70 participants responded to the survey (n = 70). Digital consent was obtained prior to voluntary survey participation with the option to withdraw at any time.

Subjects

Respondent clinicians who implant neuromodulation devices were recruited using a social media communication strategy. A link to the survey was originally posted and shared on social media sites ("X" and LinkedIn). In addition, emails were also sent via various physician community listservs in the state.

Survey Development

The survey was developed to ascertain providers' perceived knowledge regarding data privacy and cybersecurity issues in neuromodulation systems. See Supplemental Document 1 for the full survey.

Analysis

Responses were recorded in a secure, blinded REDCap database and data was analyzed using Microsoft Excel. Descriptive statistics were used to characterize the results of the survey.

Results

Seventy respondents representing pain medicine (51), neurosurgery (14) and other (5) completed the online survey (Table 1). About 52% of respondents had under 10 years of clinical experience, while 28.5% had over 15 years of experience. About 80% of respondents were male.

Table 1 Demographics of Survey Participants

Gender:	Male	Female			
	56	14			
Specialty:	Neurosurgery	Orthopedic surgery	Pain medicine	Other	
	14	1	51	4	
Years of training:	0–4 years	5–9 years	10–14 years	15–19 years	>20 years
	25	12	13	5	15

Out of the 70 participants, 69% responded that they never talk to their patients about device cybersecurity, 30% reported that they sometimes do, and only 1% responded that they always do (Figure 1). Regarding their familiarity with issues in device cybersecurity, the majority of respondents reported being not familiar (43%) and somewhat familiar (49%) and the rest (9%) said they were very familiar (Figure 2). When asked to rate their knowledge of device cybersecurity issues compared to other physicians in their field, 29% felt they were below average, 59% average, and 13% above average (Figure 3). Regarding their familiarity with issues in data privacy, the majority (61%) reported being somewhat familiar, 23% were very familiar, and 16% were not familiar (Figure 4).

Two open-ended questions soliciting comments or questions about cybersecurity and thoughts about how clinicians should address these issues were also included. A thematic qualitative analysis was conducted. Respondents noted an interest in the "big and underexplored issue", while others noted its being a low priority with few threats or had no questions or comments. There was an interest in covering the topic through medical professional education and through cooperation with device manufacturers, while some respondents were concerned about the burden of additional responsibilities for clinicians.

Discussion

To our knowledge, this is the first study to evaluate clinician knowledge on data privacy and cybersecurity issues and neuromodulation. In aggregate, the results showed that the majority of providers surveyed do not talk to their patients about device cybersecurity, and only sometimes talk to their patients about data privacy. Few trends were observed for the other survey questions as most responses tended to favor selections indicating average familiarity with the topic. Of note, those practicing for >20 years rated themselves at "average" or "above average" at a higher rate, while those

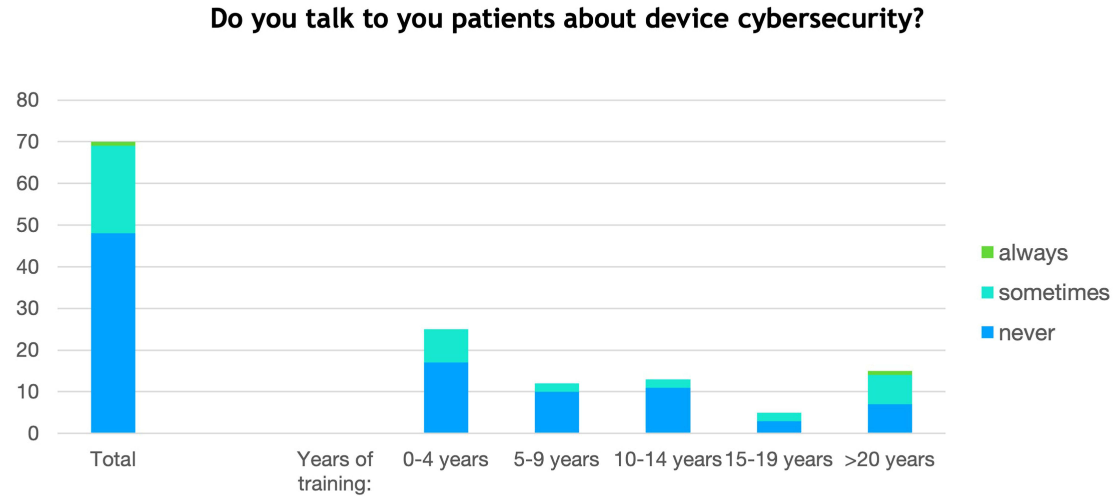

Figure 1 Patient education.

https://doi.org/10.2147/JPR.S506509

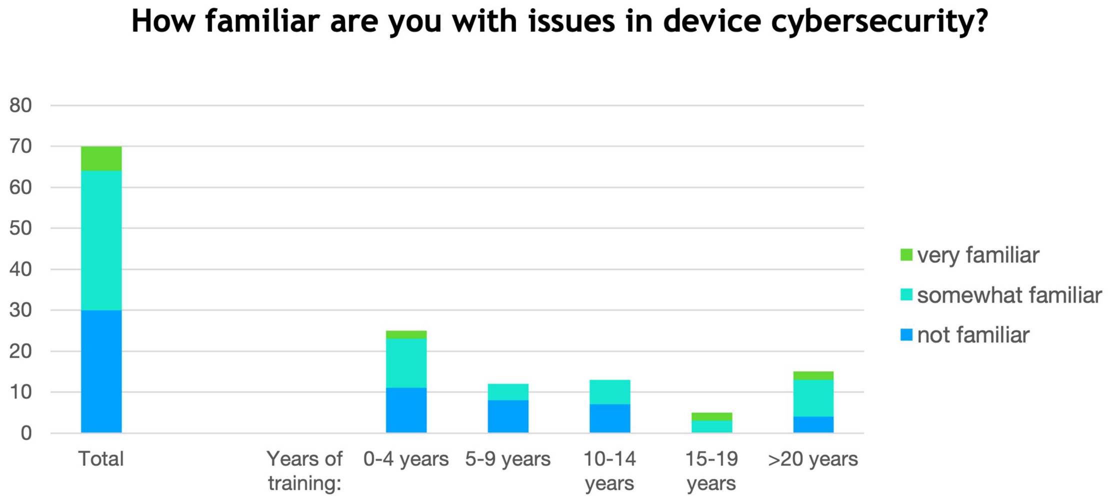

Figure 2 Familiarity with issues in device cybersecurity.

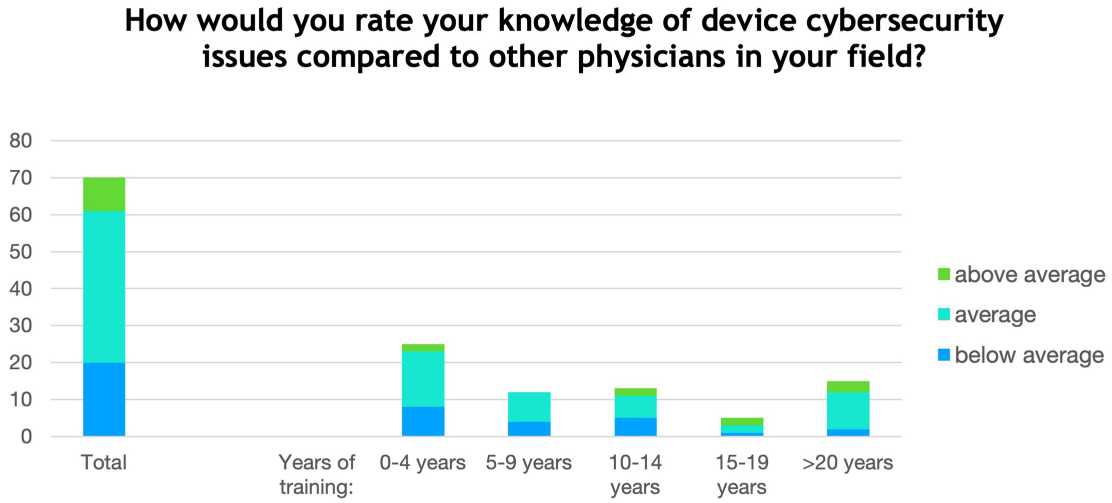

Figure 3 Knowledge of device cybersecurity issues compared to other physicians in their field.

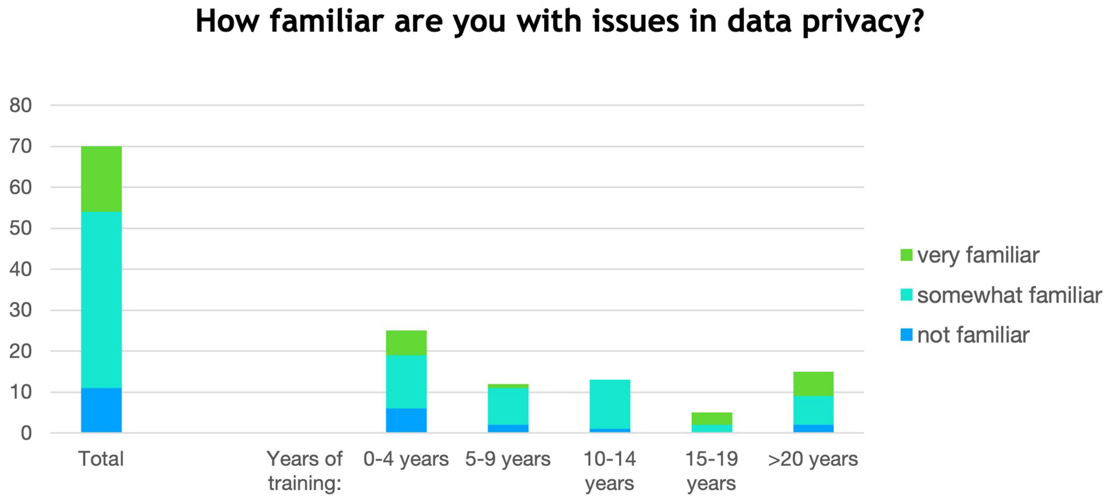

Figure 4 Familiarity with issues in data privacy.

practicing 0–4 years chose the first choice (never, below average, etc.) with a higher frequency. Also, male respondents were more likely to choose "above average" comfort with cybersecurity discussion than female respondents.

One of the limitations of an online survey is that it provides a limited perspective on a topic using primarily descriptive statistics. There is a potential selection bias in the participants who self-selected to take part in the online survey. Due to the social media method of dissemination, this survey may not have reached physicians who lack a social media or significant technology interface presence. Confounding variables also include stratification of responses based on type of institution (academic vs private) and lack of inferential analyses of the data. However, a major benefit of this format is that it allows broad dissemination and for one to gauge the interest level of neuromodulation device implanting clinicians. This is useful in establishing a baseline knowledge for these topics.

When it comes to cybersecurity, neuromodulation lags behind interventional cardiology, lacking official cybersecurity guidelines and a mechanism for knowledge dissemination to providers. In 2018, the Heart Rhythm Society released guidelines for healthcare professionals regarding how to communicate issues of cybersecurity in cardiac implantable electronic devices.[10] In 2021, the FDA released a series of educational videos for patients and the public on the topic, which has been viewed 13,133 times as of November, 2024.[6]

Data privacy and cybersecurity should both be seriously considered for all devices that interact with our patients. In the case of cybersecurity, the goal is to ensure that devices are impermeable to hacking that could alter their function or impact clinical decision-making. Consider, for instance, an implanted defibrillator whose initiation trigger might be manipulated in some way,[11] or continuous cardiac monitors that could be programmed to show incorrect rhythms.[12] The potential risks in these devices have been reported through the Heart Rhythm Society[10] and in the Journal of the American Medical Association.[13]

Patient data privacy is a key tenet of HIPAA legislation, but data acquired by devices outside the medical record may not be protected. In the case of the Apple Watch or iPhone, if Siri is voice-activated, then listening is continuous, and some of the audio has been recorded to analyze and "teach" Siri better voice recognition.[14] The Amazon Alexa device was also involved in collecting recordings of users' voices of which they were unaware.[15] Clinicians should consider disabling these voice-activated features while providing direct patient care until more is known about the privacy of discussions overheard by our mobile devices. With data breaches becoming more common, patients and clinicians should discuss the privacy implications related to using health tracking apps and technology linked to their implanted devices to protect them from phishing or other vulnerabilities.

Conclusion

Cybersecurity flaws in medical devices and software have the potential to impact the safety and security of patients and medical providers. The United States Food and Drug Administration has issued guidance on the cybersecurity of medical software and computer-connected devices. Ultimately, it is up to healthcare providers to utilize these products with the best interest of patients in mind. Clinicians who implant neuromodulation devices must understand the risks associated with their use and further how to improve overall cybersecurity to enhance patient safety and outcomes. Based on the results of this survey, both providers and patients may have limited knowledge on this subject. Our survey is the first foray into assessing the extent of healthcare provider knowledge of neuromodulation device cybersecurity and data privacy. The findings suggest that further education should be undertaken to promote the impact of these issues and to assist clinicians in educating patients about these risks.

Disclosure

Erika Petersen has received research support from Mainstay, Medtronic, Nalu, Neuros Medical, Nevro Corp, ReNeuron, SPR, Surgical Information Systems, and Saluda, as well as personal fees from Abbott Neuromodulation, Biotronik, Medtronic Neuromodulation, Nalu, Neuros Medical, Nevro, Presidio Medical, Saluda, and Vertos. She holds stock options from SynerFuse and neuro42. The abstract of this paper was presented at the North American Neuromodulation Society 26 Annual Meeting as an e-poster presentation with interim findings. The poster's abstract was published in Neuromodulation: Technology at the Neural Interface: https://doi.org/10.1016/j.neurom.2023.04.376. The authors report no other conflicts of interest in this work.

References

1. Sushant T, Sumant O. Implantable medical devices market: global forecast 2030. Allied Market Research. Available from: https://www.alliedmarketresearch.com/implantable-medical-devices-market. Accessed June 11, 2025.
2. Staats P, Deer TR, Hunter C, et al. Remote management of spinal cord stimulation devices for chronic pain: expert recommendations on best practices for proper utilization and future considerations. *Neuromodulation*. 2023;25:S1094–7159. PMID: 37632517. doi:10.1016/j.neurom.2023.07.003
3. Pycroft L, Boccard SG, Owen SLF, et al. Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurg*. 2016;92:454–462. doi:10.1016/j.wneu.2016.05.010
4. Consolidated Appropriations Act, 2023, H.R. 2617, 117th Congress, Session 2; 2022.
5. Fu K. Regulatory affairs: medical device cybersecurity. NCVHS; July 2021. Available from: https://ncvhs.hhs.gov/wp-content/uploads/2021/07/4B-Fu-rev-July-14-2021-508.pdf. Accessed June 11, 2025.
6. U.S. Food and Drug Administration. Cybersecurity awareness for connected medical devices. YouTube; 2021. Available from: https://www.youtube.com/watch?v=TU1w6fQ-yf8. Accessed June 11, 2025.
7. U.S. Food and Drug Administration. Tips for clinicians – keeping your patients' connected medical devices safe. YouTube; 2022. Available from: https://www.youtube.com/watch?v=oxLbTPdtsLI. Accessed June 11, 2025.
8. Cybersecurity in medical devices: refuse to accept policy for cyber devices and related systems under Section 524B of the FD&C Act. (n.d.) Available from: https://www.fda.gov/media/166614/download. Accessed April 16, 2023.
9. Ransford B, Kramer DB, Foo Kune D, et al. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. *Pacing Clin Electrophysiol*. 2017;40(8):913–917. doi:10.1111/pace.13102
10. Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Van Hare GF. Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians-Proceedings of the Heart Rhythm Society's Leadership Summit. *Heart Rhythm*. 2018;15(7):e61–e67. PMID: 29753946. doi:10.1016/j.hrthm.2018.05.001
11. American College of Cardiology. Can Your Cardiac Device Be Hacked? February 2018. Available from: https://www.acc.org/about-acc/press-releases/2018/02/20/13/57/can-your-cardiac-device-be-hacked. Accessed June 11, 2025.
12. Butler M. Vital sign monitors pose vulnerability to hacking. Journal of AHIMA; August 2018. Available from: https://journal.ahima.org/2018/08/21/vital-sign-monitors-pose-vulnerability-to-hacking/. Accessed June 11, 2025.
13. Kramer DB, Fu K. Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. *JAMA*. 2017;318(21):2077–2078. doi:10.1001/jama.2017.15692
14. Haselton T. Apple apologizes for listening to Siri conversations. CNBC; August 2019. Available from: https://www.cnbc.com/2019/08/28/apple-apologizes-for-listening-to-siri-conversations.html#:~:text=Apple%20on%20Wednesday%20apologized%20for,their%20Siri%20requests%20are%20handled. Accessed June 11, 2025.
15. Fowler G. Alexa has been eavesdropping you this whole time. The Washington Post; May 2019. Available from: https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/. Accessed June 11, 2025.