International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Awareness of Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey

**Ms. Priya S. Mankar[1], Mr. Aniket G. Magar[2], Ms. Arti D. Wadhai[3], Dr. Nitin H. Indurwade[4], Ms. Tejshwini A. Gaikwad[5], Ms. Sheetal K. Khobragade[6]**

[1,2,3] B. Pharm Final Year Student, Department of Pharmacy, Dr. R. G. Bhoyar Institute of Pharmaceutical Education and Research, Wardha.

[4]Principal, Department of Pharmacy, Dr. R. G. Bhoyar Institute of Pharmaceutical Education and Research, Wardha.

[5]Assistant Professor, Department of Pharmacy, Dr. R. G. Bhoyar Institute of Pharmaceutical Education and Research, Wardha.

[6]Assistant Professor, Department of Pharmacy, Dr. R. G. Bhoyar Institute of Pharmaceutical Education and Research, Wardha.

## ABSTRACT

Implantable Medical Devices (IMD'S) are advanced electronic medical devices which is surgically placed in the human body to treat medical conditions and monitor health or improve body functions. Some common examples include pacemakers, neurostimulators, drug delivery systems, and biosensors. IMD's play a significant role in managing chronic diseases and enhancing patient quality life. Due to advancement in technology the integration of IMD's into healthcare systems has transformed modern medicines and enabling continuous monitoring along with personalized care. However, IMD'S are associated with significant security and privacy challenges, such as hacking, data breaches, and interference, which can compromise patient safety. Pharmacists have critical role in addressing the safety and privacy of IMD's. They contribute by educating patients, monitoring device compliance, and collaborating with healthcare teams to implement secure practices. A survey conducted among 200 participants (including 50 pharmacists, 50 doctors, 25 IMD patients, and 75 pharmacy students) explored awareness and understanding of IMD security risks.

Among healthcare providers, 88% of pharmacists and 92% of doctors recognized the potential for security risks like hacking. However, only 32% of pharmacists and 55% of doctors consistently discuss these risks with patients. Regarding current technology, 78% of pharmacists believed IMDs are secure, compared to only 36% of doctors. Patients showed moderate awareness, with 64% being somewhat familiar with security issues, but 48% admitted they had not considered cyber threats. Pharmacy students displayed higher awareness due to academic exposure, with 58.7% somewhat familiar with the risks and 46.7% acknowledging the importance of knowing about security.

**Keywords:** Implantable Medical Device (IMDs), Security and Privacy, Hacking and Data Breaches, Patient Safety, Wireless Communication, Chronic Disease Management, FDA guidelines, ISO Standards, Healthcare Providers, Patient Education, Data Protection, Cyber Threats, Survey and Questionnaire, Health System, Privacy Concerns, Continuous Monitoring, Data Security Protocols, Pharmacy Students, Medical Practitioner, Body Area Network (BANs), Pharmacy interventions, Healthcare Collaboration, Technology Awareness, Cybersecurity Risks.

## INTRODUCTION

Implantable Medical Devices (IMDs) are electronic devices implanted within the body to treat a medical condition, monitor the state or improve the functioning of some body part, or just to provide the patient with a capability that he did not possess before [1].

Current examples of IMDs include pacemakers and defibrillators to monitor and treat cardiac conditions; neurostimulators for deep brain stimulation in cases such as epilepsy or Parkinson; drug delivery systems in the form of infusion pumps; and a variety of biosensors to acquire and process different bio signals [1].

The integration of computing devices and health care has changed the landscape of modern medicine. Implantable medical devices (IMDs), or medical devices embedded inside the human body, have made it possible to continuously and automatically manage a number of health conditions, ranging from cardiac arrhythmia to Parkinson's disease. Body area networks (BANs), wireless networks of wearable computing devices, enable remote monitoring of a patient's health status [3].

Regulatory Guidelines for IMD's
FDA (us food and drug administration
21 CFR part 820
FDA's cybersecurity Guidance (2018)
ISO Standard
ISO 14971
ISO/IEC 27001
ISO 13485

**AIM:** The aim of this survey is to assess the awareness and role of pharmacists in addressing security and privacy issues related to implantable medical devices, ensuring patient safety and data protection. It also seeks to explore pharmacy interventions that mitigate risks associated with these devices.

## OBJECTIVE:

1. To evaluate the current awareness level of pharmacists regarding the security and privacy risks associated with implantable medical devices.
2. To identify common security and privacy vulnerabilities in implantable medical devices and assess the pharmacist's knowledge of these risks.
3. To investigate the role of pharmacists in advising patients on the safe use of implantable medical devices, focusing on data protection and device security.
4. To recommend strategies for improving pharmacist education and training related to the security and privacy of implantable medical devices, ensuring better patient safety and data protection.

## IMPLANTABLE MEDICAL DEVICES

A medical device is defined as implantable if it is either partly or totally introduced, surgically or medically into the human body and is intended to remain there after the procedure[2] to continuously monitor its health, detect and predict certain conditions and deliver therapies.[8] The location where the IMD is implanted surgically depends on which health problem the physician is trying to solve[8]. For example, A patient with severe hearing loss may consent to a cochlear implant, which is surgically placed in the inner ear to provide a sense of sound.[4]

The most common types of Implantable Medical Devices (IMDs) are:

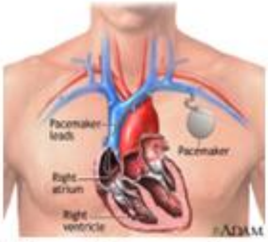


Figure 1:Pacemaker

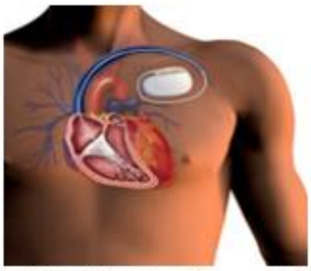


Figure2:Implantable Cardiovert Defibrillator

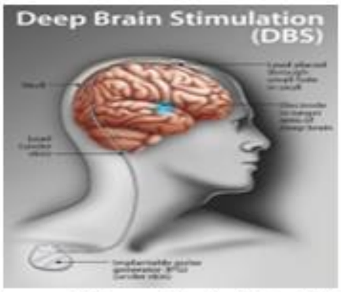


Figure 3 :Deep Brain Simulation

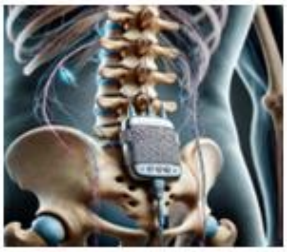


Figure 4:Spinal Cord Stimulators

Figure 5:Insulin Pump

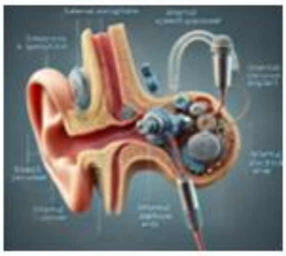


Figure 6:Cochlear Implant

## ROLE OF IMPLANTABLE MEDICAL DEVICES IN MODERN HEALTHCARE

In modern healthcare, IMDs play a crucial role by offering continuous monitoring, delivering targeted therapy, and improving the quality of life for patients with chronic conditions.[7]

1. Chronic Disease Management
2. Continuous Patient Monitoring
3. Targeted Drug Delivery and Therapy
4. Improving Patient Outcomes and Quality of Life

## PLAN OF WORK

The project will begin with a thorough review of existing research on the security and privacy risks associated with implantable medical devices (IMDs) to identify knowledge gaps and inform the survey design. A well-structured questionnaire will then be developed to assess awareness, knowledge of healthcare providers, IMD's users, pharmacy students. Along with a focus on pharmacist role in patient safety and data protection. The next step is to select a diverse group of healthcare providers from various healthcare settings, such as hospitals and community pharmacies, ensuring a representative sample. The questionnaire will be distributed online or offline to gather responses on practitioner understanding and actions regarding IMD security and awareness of patients and students. Finally, the collected data will be analyzed to identify trends, knowledge gaps, and areas where improvements are needed in pharmacist education and practices to enhance patient safety and data security for IMDs.

**Study of literature survey → Framing of questionnaire → Selection of survey area → Collection of data from the general population → Interpretation of result from the general population.**

## METHODOLOGY

Study design and population: A self-made questionnaire was distributed to 200 peoples (including 50 pharmacists, 50 medical practitioner, 25 patients, 75 pharmacy students) who agreed to participate in the study. The outcomes of this study were to evaluate the awareness, consequences, and interventions for addressing security and privacy issues in implantable medical devices.

Study procedure: Data were collected using a semi-structured questionnaire to obtain information about the awareness and role of pharmacists, medical practitioners, and pharmacy students in addressing security and privacy issues related to implantable medical devices. The questionnaire also explored the risks and pharmacy interventions associated with these devices to ensure patient safety and data protection. Face-to-face interviews were conducted with pharmacists, medical practitioners, implantable medical device users, and pharmacy students to minimize the risk of any possible misinterpretations by the participants and to avoid incomplete survey.

Location of study: The survey covered local pharmacy shops, medical practitioners in Sewagram and Sawangi hospital, and patients using IMD's in Wardha.

Study population: The study involved 200 participants, including 50 pharmacists, 50 medical practitioners, 25 patients using IMDs, and 75 pharmacy students.

Data collection method: Two separate paper-based questionnaires were administered: a 20-question form for pharmacists and medical practitioners, and a 15-question form for patients and students. The survey focused on assessing the participants understanding of security and privacy concerns associated with IMDs.

Score calculation: Each participant's responses were scored based on their level of awareness and knowledge about security and privacy issues in IMDs.

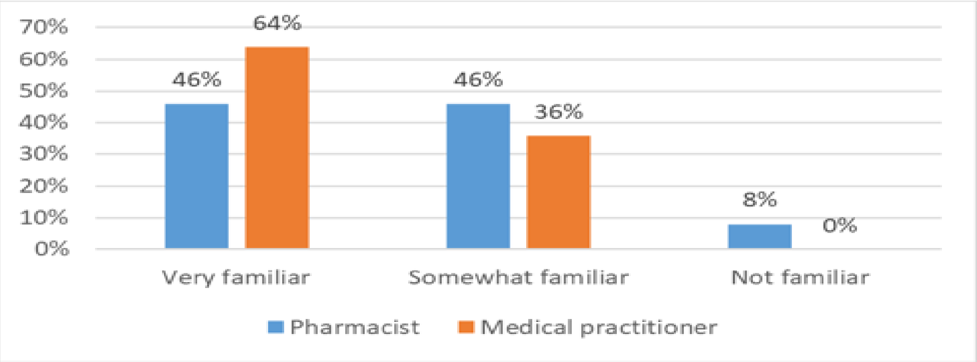
## QUESTIONS & RESULTS

### 1] Comparative Study between Medical Practitioner & Pharmacist

**1)How familiar are you with the technology behind implantable medical devices, including their wireless communication capabilities?**

**Pharmacist:** 46% very familiar, 46% somewhat familiar, 8% not familiar.

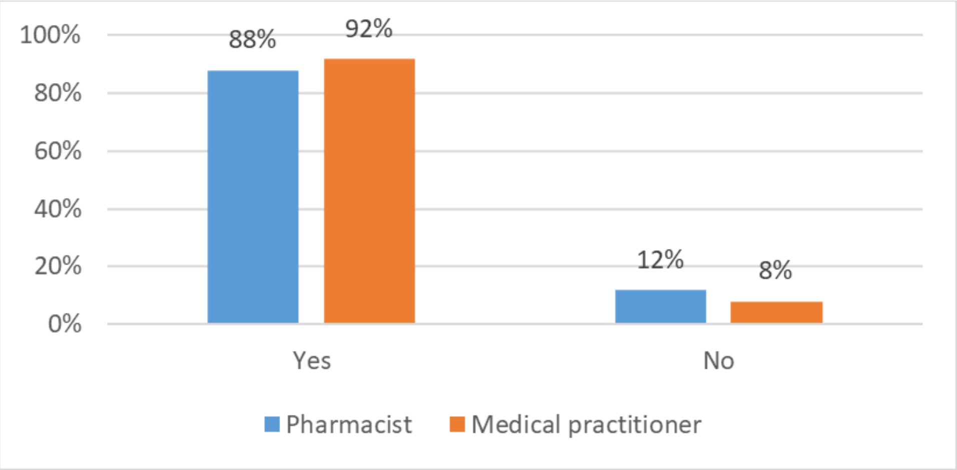
**Doctors:** 64% very familiar, 36% somewhat familiar, 0% not familiar.



**2) Are you aware of the possibility of security issues (e.g., hacking) in implantable medical devices?**

**Pharmacist:** 88% indicating a high level of concern and understanding within the profession. 12% respond no.

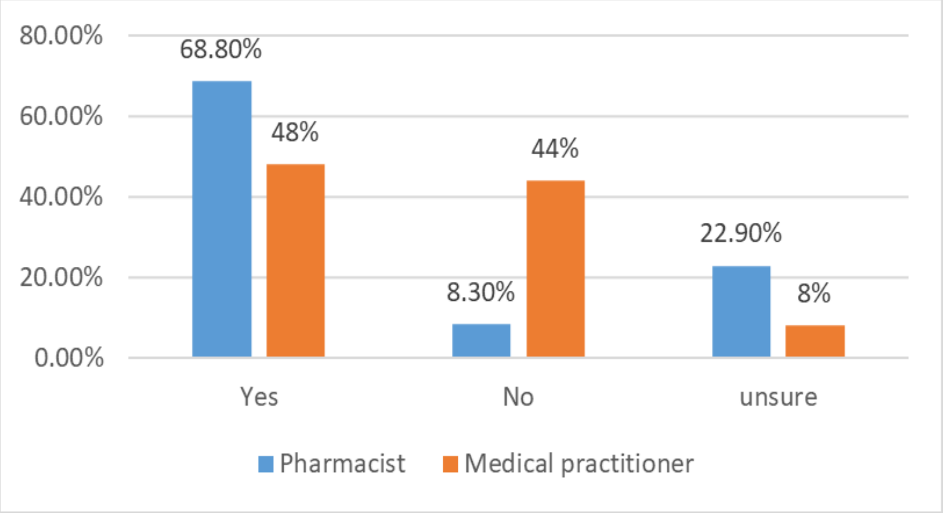
**Doctors:** 92%indicates high level of concern, 8% respond no.



**3) In your opinion, are healthcare facilities (e.g., hospitals, pharmacies) equipped to handle the security and privacy concerns of implantable devices?**

**Pharmacist:** 68.80% believed facilities are equipped, while 22.9% were unsure, and 8.3% disagreed.

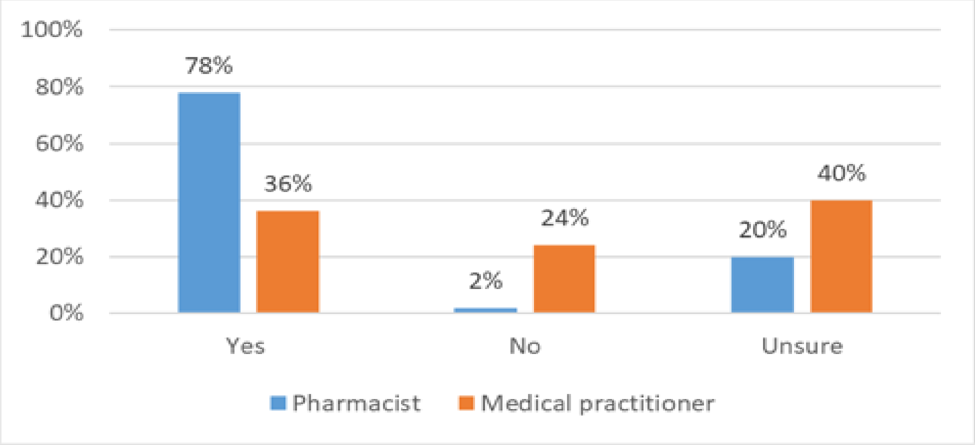
**Doctors:** 48% felt facilities were equipped, with 44% disagreeing.



**4) Do you think the current technology in implantable medical devices is secure from potential data breaches?**

**Pharmacists:** 78% of pharmacists felt the technology is secure, while 20% were unsure, and only 2% disagreed.

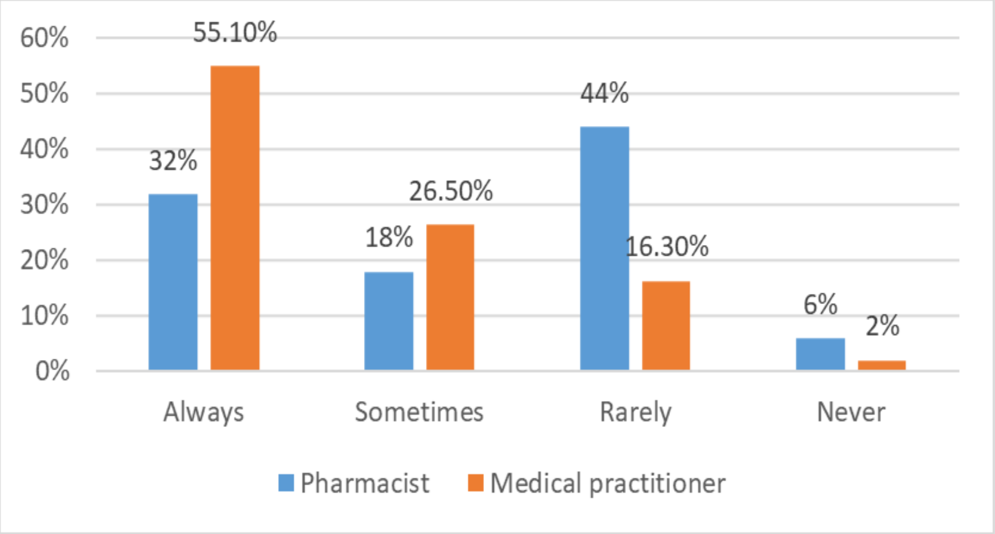
**Doctors:** Only 36% of doctors believed the technology is secure, with 40% unsure and 24% disagreed.



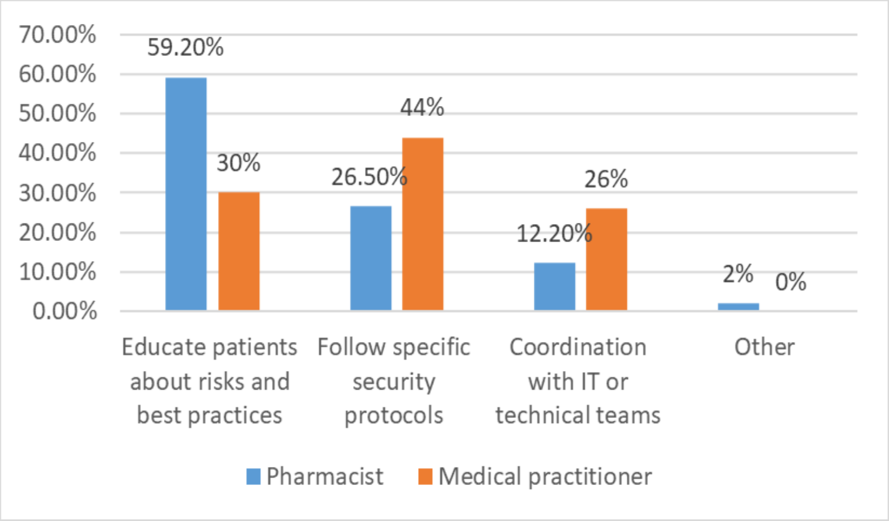
### 5) How often do you discuss security or privacy risks of implantable medical devices with your patients?

**Pharmacists:** 32% always discuss risks, while 44% rarely discuss them. This shows a significant gap in communication.

**Doctors:** 55.1% always discuss risk, 26.5% are discuss risk sometimes, 16.3 % are discuss risk rarely while 6% never.



### 6) What measures do you take, if any, to ensure the security and privacy of patient data from implantable medical devices?

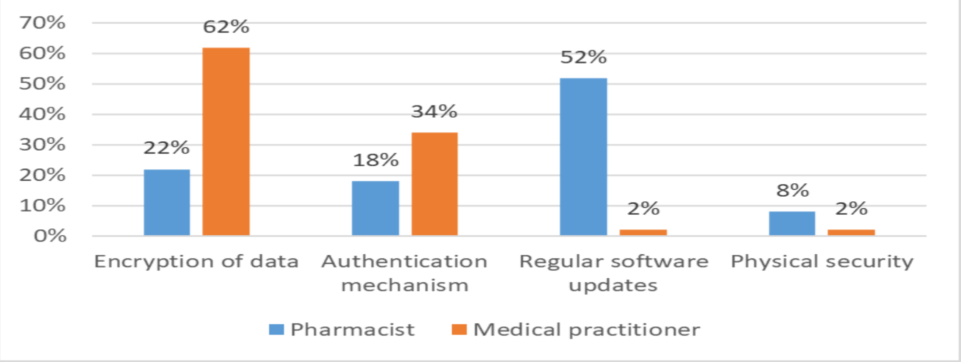


**Pharmacists:** 59.2% focus on patient education, and 26.5% follow specific security protocols, while only 12.2% coordinate with technical teams.

**Doctors:** 30% educate patients, 44% follow specific protocols,26% coordinate with technical teams.

### 7) What steps can be taken to improve the security and privacy of implantable medical devices?

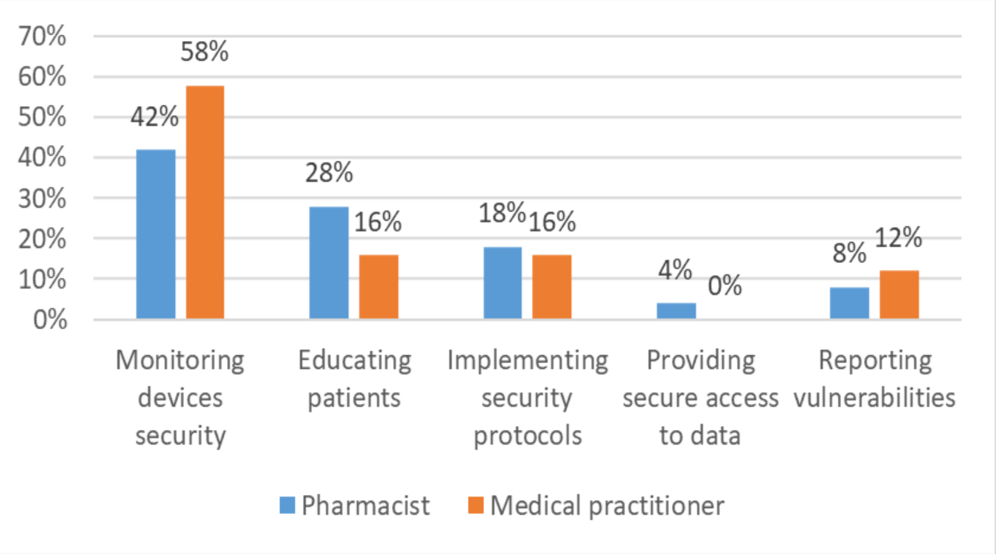
**Pharmacists:** 22% used data encryption .18% used authenticate mechanism ,52% prioritized regular software updates, while 8% used physical security. **Doctors:** 62% suggested encryption and 34% authentication mechanisms 2% regular software updates & 2% physical security.



### 8) What role do you think healthcare professionals (pharmacists, doctors) should play in addressing security and privacy issues with implantable medical devices?

**Pharmacist:** 42% monitor security, 28% educating patient, 4% provide secure access, while 8% reporting vulnerabilities.

**Doctors:** 58% monitor security, 16% educating patient, 0% provide secure access, while 12% reporting vulnerabilities.

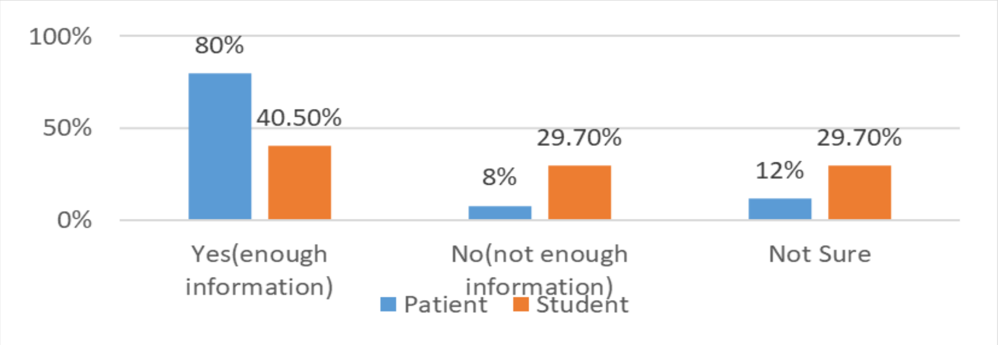


## 2] Comparative Study between IMD'S users and Pharmacy students

### 1) Do you think patients are provided enough information about the security risks of implantable medical devices?

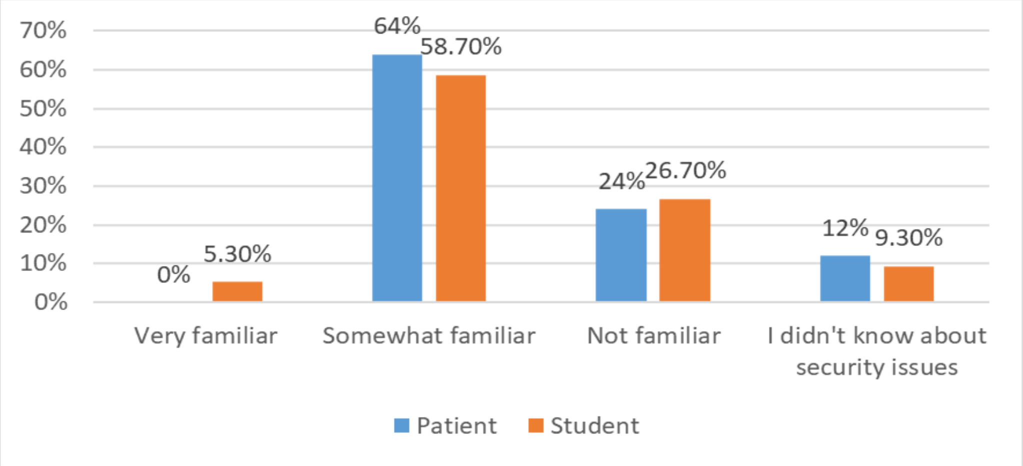
**Patient:** 80% had enough information, 8% not enough information, while 12% was not sure.

**Student:** 40.5% had enough information, 29.7% not enough information, while 29.7% was not sure.

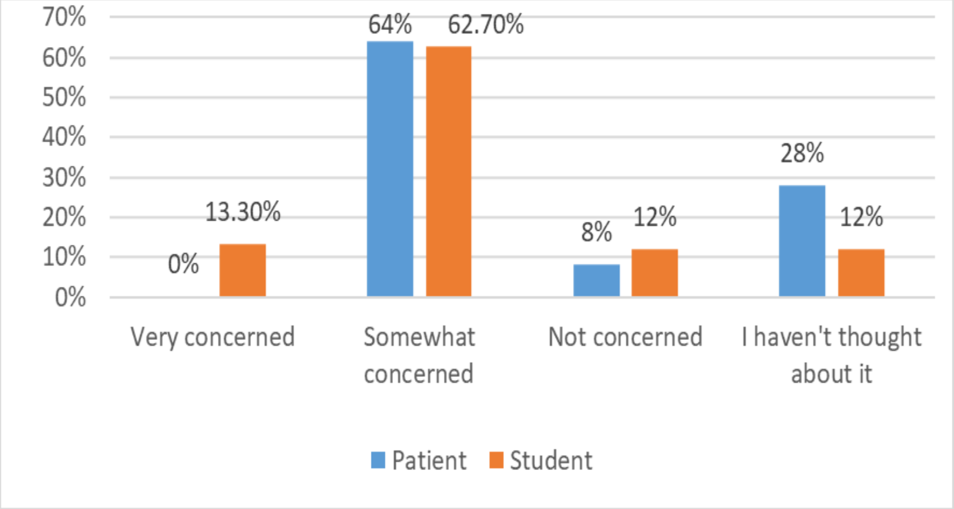


### 2) How familiar are you with security and privacy concerns related to implantable medical devices (e.g., data safety, device hacking)?

**Patients:** 64% were somewhat familiar, but 24% were not familiar, and 12% were unaware of security concerns.
**Students:** 58.7% were somewhat familiar, but 26.7% were not familiar, and 9.3% were unaware.



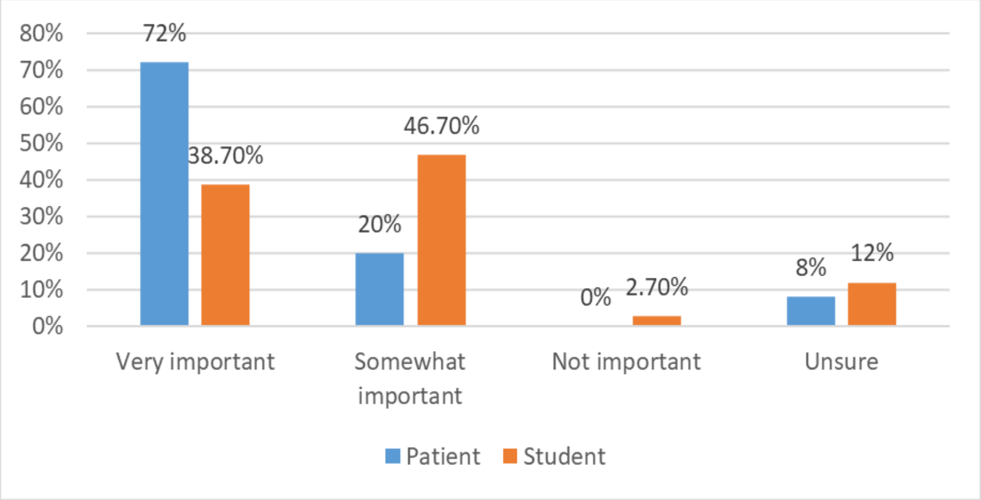
### 3) How concerned are you about the privacy and security of implantable medical devices?



**Patients:** 64% were somewhat concerned,8% not concerned but 28% had not considered it.

**Student:** 13.3% were very concerned, with 12% unconcerned.

### 4) How important do you think it is to know about the security and privacy aspects of implantable medical devices?



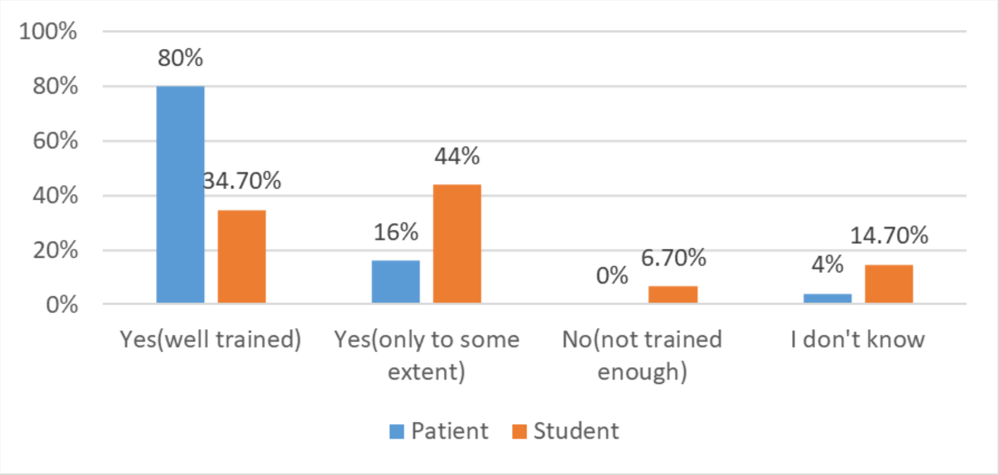
**Patients:** 72% believed this was very important, 20% somewhat important, 8% unsure.

**Students:** 38.7% felt it was very important, 46.7% somewhat imp, 2.7% not imp, 12%unsure.

### 5) Do you believe healthcare providers are trained to address security and privacy concerns about implantable medical devices?

**Patients:** 80% were believed healthcare providers were well-trained, 16% considered to some extent, 4% unsure.

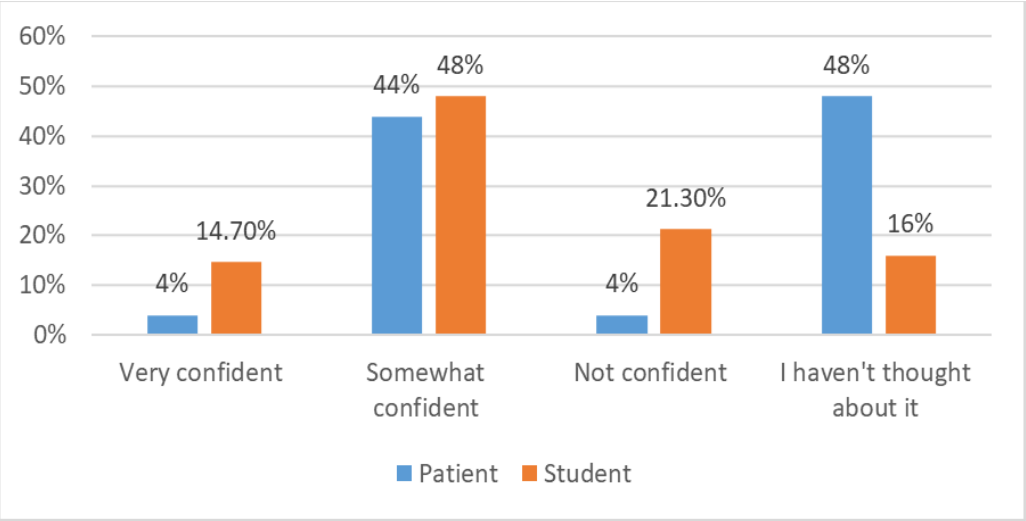
**Students:** Only 34% believed they were well-trained, with 44% to some extent, 6.7% no, 14.7% unsure.



### 6) How confident are you that implantable medical devices are safe from cyber threats or hacking?

**Patients:** 44% were somewhat confident but 48% had not thought about it, while 4% very confident & not also.

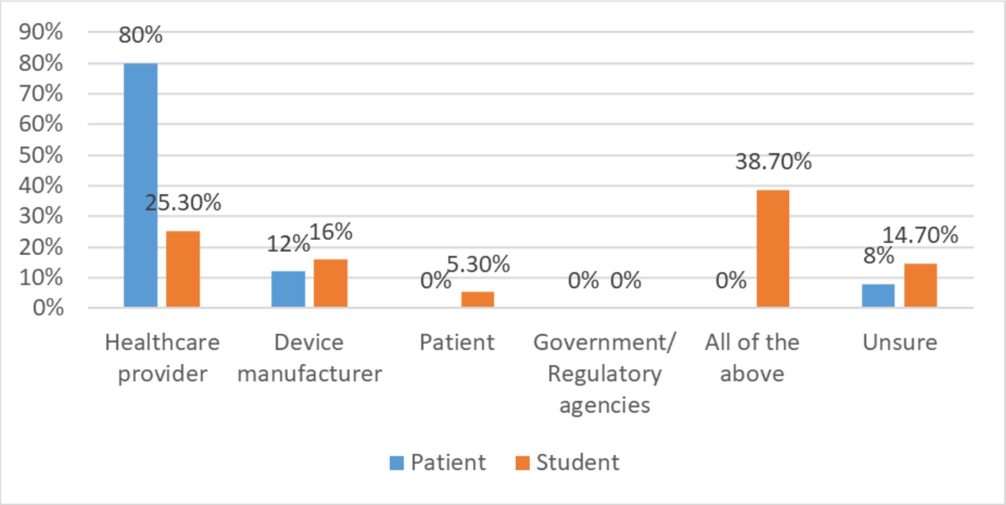
**Students:** 48% somewhat confident but 21.3% not confident, 14.7% very confident, 16% unsure.



### 7) In your opinion, who should be responsible for ensuring the security and privacy of implantable medical devices?

**Patients:** 80% healthcare providers, 12% manufacturer, 8% unsure.

**Students:** 38.7% believed all stakeholders while 16% manufacturer, 14.7% unsure, while 5.3% consider patient are responsible.



## DISCUSSION

The survey shows that people have different levels of understanding and opinions about the security and privacy risks of implantable medical devices (IMDs), especially among healthcare providers, patients, and students. Among healthcare providers, both pharmacists and doctors generally understand how IMDs are used in treatment, particularly in customizing patient care and monitoring health over time. While both groups recognize the potential security risks, like hacking or unauthorized access, doctors appear to discuss these risks with patients more often than pharmacists.

Pharmacists, for their part, are familiar with IMD technology, and many acknowledge the importance of managing security risks, though there seems to be some uncertainty about their specific role in preventing these risks. This may be reflected in the lower frequency of privacy discussions pharmacists have with patients compared to doctors. A good number of pharmacists focus on educating patients about security, but many also rely on IT support and established security protocols. Patients and students have a moderate understanding of IMD security concerns. Students tend to be more aware of these issues due to academic exposure, while patients rely mostly on their healthcare providers for information. Although patients generally recognize that security and privacy are important, they lack specific knowledge, highlighting the need for clearer, more accessible information.

## CONCLUSION

This study underscores a gap in consistent patient education regarding IMD security and privacy. Healthcare providers, especially pharmacists, could play a more active role in educating patients about these risks. Although healthcare providers are aware of the potential security issues, a stronger emphasis on protocols and closer collaboration with IT departments could enhance data security. For patients and students, improved education on security measures and privacy best practices could be beneficial. Addressing these areas could help patients feel more confident in using IMDs, reduce the risk of security breaches, and create a safer environment overall.

## ACKNOWLEDGEMENT

We are thankful to Almighty for giving me strength to complete my Practice School successfully. We sincerely wish to express our gratitude to the **Dr. R. G. Bhoyar Institute of Pharmaceutical Education & Research, Wardha Affiliated by Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur** for providing all the necessary resources and facilities for completing our Practice School.

First of all, we are grateful to the Director of our college for providing the college facilities to the successful completion of practice School of each department and his kind patronage.

We owe our sincere gratitude to **Dr. Nitin Indurwade Sir** Principal of **Dr. R. G. Bhoyar Institute of Pharmaceutical Education & Research, Wardha Affiliated by Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur** for the perfect guidance. His guidelines and instructions were really helpful for learning and completing all modules on time. We would like to thank our friends who were in the of Practice School. Their kind support and cooperation throughout the semester. We are really grateful to the loving parents and family members for being an inspiration and great support for us. The satisfaction and joy of completing our practice School would not be complete without expressing our gratitude to these people who made it possible because success only came through high ambition, strong effort, good guidance and encouragement.

## REFERENCE

1. Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador, “Security and privacy issues in implantable medical devices: A comprehensive survey”, (2015) 272-289.
2. Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, SoK: “Security and Privacy in Implantable Medical Devices and Body Area Networks”, (2014) 123-138.
3. Joung Y. H, “Development of implantable medical devices: from an engineering perspective, International neurourology journal”, (2013) 98.
4. AlTawy R., Youssef A. M, “Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices, IEEE Access”, 4, (2016) 959–979.
5. P. Bagade, A. Banerjee, J. Milazzo, S. K. S. Gupta, “Protect your BSN: No handshakes, just namaste!” in IEEE International Conference on Body Sensor Networks (BSN), (2013), pp. 1–6.
6. Ren, Y., Werner, R., Pazzi, N., Boukerche, “A. Monitoring patients via a secure and mobile

healthcare system. IEEE Wireless Communications", (2010), 59-65.

7. Eduard Marin, "Security and Privacy of Implantable Medical Devices".
8. https://imec-publications.be/handle/20.500.12860/31288, (2023)
9. Emmanuel Kwarteng, Mumin Cebe (2022): "A Survey on Security Issues in Modern Implantable Devices: Solutions and Future Issues".
10. https://arxiv.org/abs/2205.00893, (2022)
11. Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, William H. Maisel. "Security and Privacy for Implantable Medical Devices", 2008.
12. W. Burleson, S. S. Clark, B. Ransford, K. Fu, "Design challenges for secure implantable medical devices, in Proc.49th Annual Design Automation Conference" (DAC'12), 2012 pp. 12-17.