Brazilian Journal of Psychiatry
bjp
Revista Brasileira de Psiquiatria
Brazilian Psychiatric Association
Fully open access
No APCs

BJP PRE-PROOF
(article published as accepted)

Special Article

Ethical issues in implantable medical devices: future of care or Orwellian nightmare?

Fábio Augusto do Prado Marmirolli, Anna Paula Soares da Silva Marmirolli, Thiago Marques Fidalgo

http://doi.org/10.47626/1516-4446-2026-4885

Submitted: 14-Feb-2026

Accepted: 27-Jun-2026

BJP PRE-PROOF

This is a preliminary, unedited version of a manuscript that has been accepted for publication in the Brazilian Journal of Psychiatry. As a service to our readers, we are providing this early version of the manuscript. The manuscript will still undergo copyediting, typesetting, and review of the resulting proof before it is published in final form. The final version may present slight differences in relation to the present version.

Ethical issues in implantable medical devices: future of care or Orwellian nightmare?

Running title: Ethical issues in Implantable Medical Devices

Fábio Augusto do Prado Marmirolli[1], Anna Paula Soares da Silva Marmirolli[1], Thiago Marques Fidalgo[1]

[1]Department of Psychiatry, Escola Paulista de Medicina, Universidade Federal de São Paulo, São Paulo, SP, Brazil.

Correspondence: Anna Paula Soares da Silva Marmirolli – 55 11 97964-9350 – anna.p.ss@hotmail.com

ABSTRACT

Objective: Implantable medical devices (IMDs) increasingly integrate continuous monitoring with autonomous therapeutic functions, transforming clinical practice while raising significant ethical concerns. As these technologies expand – particularly among vulnerable populations such as individuals with substance use disorders – the tension between patient safety and autonomy intensifies. This article examines the ethical and legal implications of IMDs, emphasizing ongoing consent, data governance, and neurorights.

Methods: We conducted a narrative and normative bioethical analysis grounded in interdisciplinary literature. Empirical and conceptual studies on IMDs, neurotechnologies, and opioid overdose interventions were reviewed alongside regulatory frameworks, including the European General Data Protection Regulation (GDPR), Brazil's General Data Protection Law (LGPD), and the United States Health Insurance Portability and Accountability Act (HIPAA).

Results: Highly autonomous IMDs challenge traditional informed consent models, particularly regarding revocation, device deactivation, and continuous data processing. Vulnerable populations may face stigma and expanded secondary uses of sensitive data, while existing regulations leave gaps in neural and biometric data protection.

BJP PRE-PROOF

Conclusions: Ethical implementation requires patient-centered frameworks ensuring ongoing consent, secure data governance, and protection of mental privacy.
Keywords: Informed consent; data protection; neurotechnology; neurodata.

INTRODUCTION

The promise of life-saving Implantable Medical Devices (IMDs) comes with a crucial dilemma: as the devices designed to care for us grow more autonomous, the people they are meant to serve can become less so. This article emphasizes that for vulnerable populations, such as people who use opioids, this tension is acute. The necessity of device implantation, coupled with their automatic function, challenges notions of ongoing consent and individual freedom, demanding that research moves beyond engineering to embrace bioethics and the protection of sensitive personal data.

The path forward must be guided by a new era of patient protection in neurotechnology, establishing frameworks that ensure consent can be revoked, that data privacy is inherent to the device's design, and that “neurorights” are protected to guarantee the confidentiality and mental privacy of users. Without these safeguards, the future of medicine may, ironically, compromise the very freedom it seeks to preserve.

THE RISE OF IMPLANTABLE MEDICAL DEVICES

The use of implantable medical devices (IMDs) is an emerging matter, with growing importance in both the research community and clinical practice. There are hundreds of devices being designed and produced to match different health necessities. Everyone is looking to develop smaller, more efficient batteries[1], the best AI algorithms for decision making, and the most autonomous and imperceptible devices to measure and record vital signs and, in some cases, treat patients automatically[2].

In psychiatry, these developments are particularly salient. Implantable and neuromodulatory devices such as deep brain stimulation (DBS) have already been explored in treatment-resistant depression and obsessive-compulsive disorder[3],[4]. Emerging proposals also consider implantable systems aimed at preventing relapse or detecting physiological correlates of substance use[5]. Although these ideas are still in a mostly conceptual stage, there is enthusiasm around the use of Deep Brain-

BJP PRE-PROOF

Machine Interfaces (DBMI) for detecting biomarkers related to substance use disorders and using the therapeutic effects of deep stimulation, similar to the effects of DBS, in other psychiatric contexts. The recent results on Vagus Nerve Stimulation (VNS) in depressive disorders[6] bring even more expectations on these approaches.

In these contexts, the intersection between mental health, decision-making capacity, and technological intervention becomes especially complex, requiring psychiatrists to navigate not only therapeutic efficacy but also evolving standards of consent, autonomy, and long-term patient follow-up.

However, would not the most autonomous device create the least autonomous patient?

The range of IMD is now already very diverse. Published technologies for remote patient monitoring exist across different health areas, especially heart disease, dementia, pain assessment, hypertension, and other chronic diseases[2]. When it comes exclusively to invasive devices, cardiac implantable devices stand out due to the number of studies on this matter and the variety of technologies available for use[8]. Since the introduction of pacemakers in the 1960s, the number of cardiac devices has grown, with implantable cardioverter defibrillators (ICDs) among the most cited in the field of IMD, along with deep brain stimulation[9] and cochlear and glaucoma implants[10].

These devices, along with those under development, aim to perform three main activities: remotely monitoring health signs and biomarkers, alerting health professionals, families, and the patient about acute health events, and, in some cases, treating emergencies. The classic example of this last feature is the cardioversion performed by ICDs in a person presenting with a malignant arrhythmia[6]. Still, there are other present and future possibilities, such as nano pumps that deliver insulin based on the patient's glucose level[11] or ocular devices with sustained-release drug delivery to treat glaucoma[12].

To illustrate this functional architecture, Figure 1 organizes these three layers schematically, mapping current clinical examples onto each level and making explicit how monitoring, detection, and intervention build upon one another in increasingly autonomous ways:

BJP PRE-PROOF

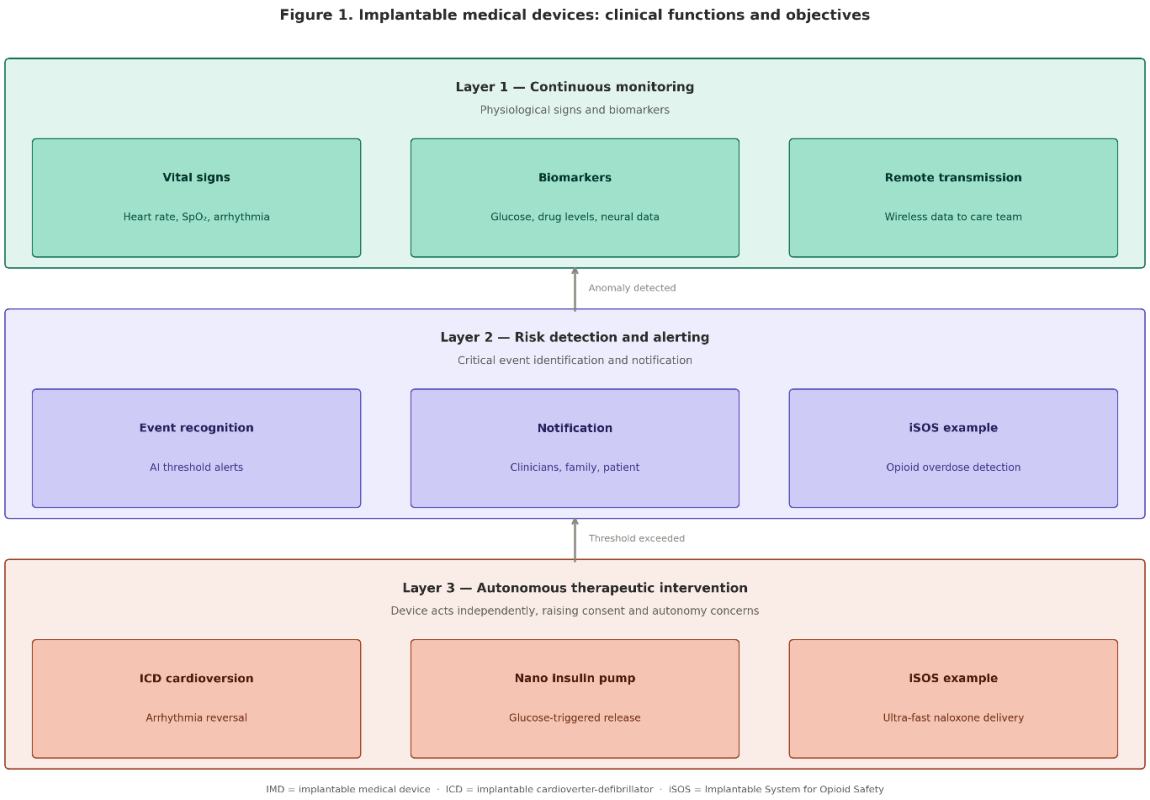


Figure 1. Implantable medical devices: clinical functions and objectives. IMDs operate across three interdependent layers – continuous monitoring of physiological signs and biomarkers, automated risk detection and alerting, and autonomous therapeutic intervention – illustrated here with current clinical examples, including cardiac devices, nano insulin pumps, and the iSOS opioid reversal system.

BJP PREP

Although these technologies are novel and have potential benefits, since their introduction, there have been ethical concerns involving their use. Some of the most recent concerns revolve around the data protection of the health information collected by the devices[13]. The ethical debate actually started to spark after these devices began actively performing tasks (treating the patient) beyond just monitoring and alerting – an editorial in the Journal of Medical Ethics from 2007[10] already argued for the ethical issue of deactivating and removing an ICD – an issue further addressed in ethical research[11].

To address this issue, we selected a case of IMD applied to the context of substance use disorder to explore the ethical consequences of this and similar devices. Based on the dilemmas of patient autonomy arising from this example, we conducted a discussion drawing on ethics and medical literature, aiming to expand the debate on this issue. This process included a literature review of both medical

science-indexed databases and regulatory instruments and legal frameworks from different countries, to encompass an integrated interdisciplinary approach.

IMPLANTABLE SYSTEMS FOR OPIOID SAFETY: A CASE STUDY IN VULNERABILITY

The ethical issue surrounding devices that treat patients based only on consent given on the date of their implantation and patient autonomy becomes even more relevant when applied to populations even more vulnerable, like people with substance use disorders (SUDs). One example of this case is the Implantable System for Opioid Safety (iSOS)[15], an implantable subcutaneous system designed for the detection and reversal of opioid overdoses. The device, designed for implantation in the subcutaneous tissue, continuously monitors respiratory rate, heart rate, heart rate variability, body temperature, and blood oxygen saturation. Its algorithm evaluates changes in these physiological parameters in real time to detect the presence of an opioid overdose and triggers an ultra-fast naloxone delivery mechanism, administering a 10 mg dose within 10 seconds of detection. According to the authors[13], the algorithm was developed through targeted research to identify the optimal balance between the accuracy of vital-sign monitoring for overdose detection and the sensors' power consumption. Prior to naloxone administration, the device also emits an alarm, vibrates, and sends an alert to the user's smartphone, allowing the process to be interrupted in the event of a false-positive overdose detection.

This specific device was selected to illustrate the present discussion because overdose reversal technologies constitute the primary area of application for implantable devices in Opioid Use Disorder. Other implantable treatments, such as spinal cord stimulation, although promising for reducing opioid use in patients with chronic pain, have thus far demonstrated limited effectiveness in achieving sustained reductions in opioid consumption[14]. Within the broader field of Substance Use Disorders, there is growing interest in Brain–Computer Interface technologies, including deep brain interfaces; however, research in this area remains largely at the conceptual stage[5].

This example is so prominent because of the recent impact of opioid overdose deaths in the United States[16], along with the effect of opioid overdose in patients capacity and autonomy, which has been thoroughly elaborated by Marco[17] in his

BJP PRE-PROOF

analysis of the research by Marshall *et al.*[18] and Joseph *et al.*[19]. These works address significant complications of opioid overdose, ranging from biological issues such as arrhythmia, infections, and thrombotic events to psychosocial challenges like SUDs, homelessness, and unemployment[18]. Furthermore, the authors note that patients often request early discharge after hospitalization due to an overdose resuscitation, given that they generally exhibit fear of retaliation, distrust in the medical institution, feelings of shame or embarrassment, fear of loss of confidentiality, and many others. The study by Joseph *et al.*[19], in turn, highlights the complex challenge of balancing beneficence and autonomy within the scope of opioid treatment, considering the possibility of erroneously presuming that the patient lacks capacity in cases where they disagree with critical medical decisions.

In a study conducted by Biernacki et al.[20], the decision-making deficit observed in opioid users, as compared with non-drug-using controls, was found to be moderate to large. This finding confirms that, when faced with choices, these individuals experience difficulty avoiding risky decisions and forgoing short-term gains in favor of larger long-term rewards.

This meta-analysis conducted by Biernacki et al. further suggests that impaired decision-making in opioid users may predict risky sexual behaviors and may also be associated with poorer treatment outcomes, including treatment dropout and higher relapse rates. Taken together, the studies included in the meta-analysis provide consistent evidence of significant deficits in decision-making among opioid users. At the same time, they do not support a categorical conclusion that opioid use invariably leads to impaired decision-making, nor do they establish a definitive causal relationship. Importantly, current research indicates that deficits in decision-making can persist even after drug use has ceased, potentially increasing the risk of relapse in individuals with opioid use disorder.

As the literature demonstrates, consent in the context of substance use disorders is highly variable and contingent on the patient's clinical state – fluctuating across periods of abstinence, craving, and intoxication, raising legitimate questions about whether consent obtained under certain of these conditions can be considered fully valid. This instability in decisional capacity may, in turn, contribute to poor treatment adherence, compromising both continuity of care and clinical outcomes, while also placing significant demands on the therapeutic relationship and on the physician's ability to manage these patients over time.

BJP PRE-PROOF

In the context of implantable devices, this fluctuating consent and the broader challenge of shared decision-making become even more salient. The implantable and autonomous nature of these technologies makes it essential that physicians provide patients – to the extent of their comprehension – with all information necessary for adequate consent. Moreover, given that the device remains active beyond the moment of implantation, this process cannot be treated as a one-time event: sustained and continuous attention to consent is required throughout the course of treatment, even – and perhaps especially – when fluctuations in the patient's decisional capacity or expressed wishes introduce new challenges along the way.

When discussing specific devices – such as wearable or semi-implantable ones – that focus on detecting reliable changes in physiology, it is possible to identify problems such as low patient adherence due to difficulty removing the device, false-positive detection, slow administration, and the engineering required to develop acceptable devices. In this context, it is notable that IMDs require constant patient follow-up, as patients may sometimes miss appointments, fail to refill medication, and fail to recharge the battery. It is also necessary to understand how the patient will cope with the device's size, which may sometimes be visible to others, and how they will respond to the audible alarm in some IMDs. In the case of people with substance use disorders, such issues may be even more sensitive, as they can further contribute to the stigma to which these individuals are typically subjected, given their particularly vulnerable position in society. A scoping review of Lyzwinski *et al*.[21] focusing on people who use opioids' perspectives on the use of wearable monitoring technology showed that privacy and the protection of personal information were two of the biggest concerns for the use of these devices – this may be an even greater issue when it comes to implanted devices. The same review also discusses concerns about the use of wearable devices due to the fear of making law enforcement suspicious.

Building on this example, there are several questions researchers should consider about IMDs in general: once implanted, how easily could they be removed? What level of control does the user have to deactivate the device? What are the impacts of automatic data capture and battery limitations on the patient's relationship with their doctor? How would the system ensure that only an authorized user's mobile device can connect to these devices? What if the user loses access to the

BJP PRE-PROOF

authorized device? How can the handling of this application by unauthorized third parties be prevented? How would the selection of the authorized user or third party to activate the device be carried out? If the device operates autonomously, what is the possibility of turning it off? And if such a shutdown affects the user's treatment?

Considering the inherent limitations of IMDs – such as restricted energy, storage, and processing capacity – security solutions must strive to achieve a careful balance between maintaining patient safety, protecting data, and preserving both device functionality and battery life. Moreover, both the patient and their family members should be aware of the possibility of device failure – for instance, in the detection of overdose or in drug administration – and should seek immediate hospital care in more severe cases.

INFORMED CONSENT AND CONTROL MECHANISMS

The first solution to some of these situations is an adequately informed consent process. In this context, it is evident that patients who choose to use any implantable device must be thoroughly informed about its limitations, such as the need to attend periodic medical appointments, possible refilling of the medication and/or the device itself, as well as general precautions regarding data that unauthorized third parties may potentially access. The specificity and particularity of this consent must be reflected in the informed consent form, which should be drafted with all these detailed concerns regarding future possibilities of IMD use in mind. On the other hand, regarding the IMDs connected to mobile devices, it should be noted that the protocol must comply with critical and operational security standards. The pairing process, for example, must adhere to secure configurations, such as a unique code or QR code scanning, that ignore all connection attempts from any device not on this approved list.

Given the longitudinal and technologically mediated nature of IMDs, traditional one-time consent models may be insufficient. A dynamic consent approach, also referred to as a consent continuum[22], allows ongoing communication, periodic reaffirmation, and structured mechanisms for revocation. Such features more accurately reflect the continuous data collection and autonomous functionalities of these devices. In psychiatric populations, where decisional capacity may fluctuate over time, adaptive consent frameworks may help preserve patient agency while maintaining therapeutic continuity.

BJP PRE-PROOF

In IMDs that administer medication, the device must be designed to ensure that only a predetermined and authorized device can initiate medication administration, thereby preventing accidental or malicious activations. For these IMDs that monitor and control drug administration, it is necessary to discuss how to handle situations in which the patient cannot exercise control independently and whether a family member could be authorized to assume this control. Such a scenario would certainly depend on the patient's initial consent, but questions arise regarding the duration of that consent and the mechanisms for revoking it. The withdrawal of consent, furthermore, also relates to the complexity of placing and removing the device, which will require some structure from the responsible physician. On the other hand, this situation will certainly not be able to keep up with the ups and downs of a treatment that, in the case of SUDs, is often doomed to non-adherence in a large number of patients, as well documented in the literature[18].

From an information security perspective, we should also consider the concern about how the data collected by the device will be handled. Will the attending physician receive such data regardless of the patient's consent or attendance? Can family members, employers, and other people related to the patient request such data? Can insurance companies and the government itself monitor patients for purposes that do not serve their interests? What criteria will be used for data deletion? And in the event of treatment withdrawal and/or consent withdrawal? Furthermore, in cases of treatment continuity with another doctor or other related situations, such as insurance change, how can we ensure that people who previously could access the information can no longer do so?

The rapid pace of new IMDs' emergence underscores the need for an increasingly in-depth discussion of their computing capacity, autonomous decision-making, and the particularities of wireless communication and data retention. However, such innovations also introduce significant security and privacy risks that may compromise not only the proper functioning of the implant but also the patient's health. Therefore, it becomes essential to adopt, from the earliest stages of development, the principles of privacy by design and privacy by default, ensuring that the protection of privacy and sensitive data is embedded within the system's architecture rather than treated as an afterthought[23]. In this context, "privacy by design" refers to incorporating data protection from the very creation of the system,

BJP PRE-PROOF

while "privacy by default" means that the system must be configured for the highest level of privacy from the first use, without the need for additional settings.

A comparative analysis of regulatory approaches suggests that this is an evolving and still unsettled field. From a European perspective, it is also essential to cite the GDPR (General Data Protection Regulation), which regulates data processing in the European Union and served as the basis for legislation in other countries, such as Brazil, which enacted its Lei Geral de Proteção de Dados (LGPD) in 2018. Under the GDPR, health data is a special category of data (sensitive data) and requires a more rigorous legal basis for processing. Among these, explicit consent stands out, which, according to the regulation, must be provided through a specific, informed, freely given, and unambiguous authorization. Within the scope of the GDPR, the concepts of privacy by design and privacy by default are central pillars of the regulation. They require that privacy be incorporated from the very conception of a product, implying that researchers in Neurotechnology and Brain-Computer Interfaces (BCIs) must have this concern from the outset of their research.

Despite its broad scope and its status as one of the most comprehensive protections from a data protection standpoint, the literature already points out that the exact nature of some technologies is not always precise and may fall outside the scope of GDPR protection. On this matter, in an article that examines the application of the regulation to neurotechnologies[24], the authors point out that some devices may be classified as “wellness devices” to avoid much stricter requirements, even though the data they use could be considered biometric or biomedical data. The authors argue, in this context, that neural data are a special type of data, and that the GDPR is not clear and does not distinguish between different levels of data sensitivity or the potential for personal data to be revealed through processing, overlooking the fact that data from BCIs and other brain recordings are often personal and are as sensitive as health data.

On the other hand, in the United States, the federal legislation that governs this matter is the HIPAA (Health Insurance Portability and Accountability Act) and its subsequent amendments, a foundational law for health data privacy. It applies to health insurances, healthcare providers, and data processing centers, such as laboratories, as well as to device manufacturers when they act as 'business associates' for covered entities. The regulation aims to protect so-called PHI (Protected Health Information) and does not require explicit consent for most

BJP PRE-PROOF

treatments, but it states that general consent is not sufficient to authorize the disclosure of health data to third parties; a specific, explicit, and written authorization is required. Under HIPAA, the patient has the right to revoke their authorization at any time.

Despite being an important regulatory instrument and still adequate for protecting health information in the era of Big Data, the literature[25] already points to the need to expand HIPAA to cover a broader range of entities and data, or even to create a separate framework for health-related data that falls outside HIPAA's scope, possibly inspired by the GDPR. The authors further indicate that such a revision should balance privacy protection with the facilitation of research, enhance individual control over data, and hold accountable those who misuse information. In this context, they emphasize that the concept of "health data" must be updated to reflect the digital age – something especially relevant to the debate on neurotechnologies and implantable medical devices, which generate biometric and neural data that is often beyond the reach of current legislation.

In general, entities under HIPAA's purview must implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of data. Ideally, they must observe the concepts of privacy by design and privacy by default[26], so that their IMDs do not eventually have to be adapted to legal determinations, which may also have to observe specific protections at the state level, such as the legislation of the State of California, regulated by the CCPA (California Consumer Privacy Act) and the CPRA (California Privacy Rights Act) and Colorado CPA (Colorado Privacy Act).

NEURORIGHTS AND THE PROTECTION OF MENTAL PRIVACY

From a bioethical standpoint, a key concern is that neurotechnologies such as BCI and neuromonitoring devices are advancing rapidly, and a new frontier of human rights is emerging: neurorights. These rights aim to protect mental privacy, personal identity, free will, and equitable access to mental capacity against potential misuse. The ethical challenges raised throughout this article do not operate in isolation. As summarized in Figure 2, autonomy, ongoing consent, data privacy, neurorights, stigma, and algorithmic bias form an interconnected web of tensions, all converging on the patient – whose rights and vulnerabilities remain at the center of any responsible framework for IMD implementation:

BJP PRE-PROOF

Figure 2. Key ethical dimensions of implantable medical devices and their interrelations

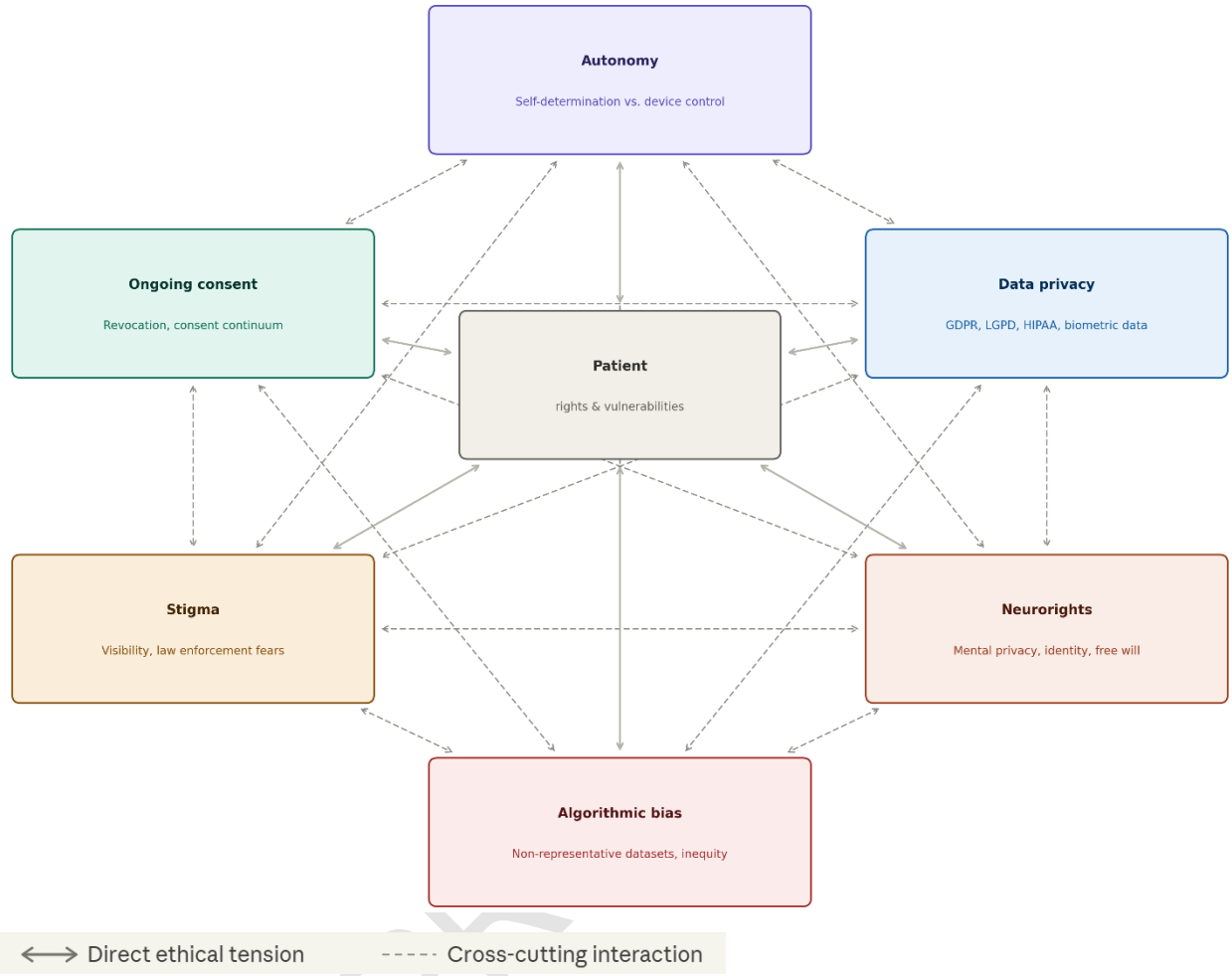


Figure 2. Key ethical dimensions of implantable medical devices and their interrelations. Patient rights and vulnerabilities occupy the center of an interconnected ethical landscape in which autonomy, ongoing consent, data privacy, neurorights, stigma, and algorithmic bias mutually reinforce and constrain one another.

In a comprehensive study on the subject, Goering and Yuste[27] present significant philosophical reflections, including the possibility of a substantial change in the concept of the self and the dissolution of traditional notions of identity, given neural activity's ability to control devices beyond our bodies. Moreover, the authors point out the risk of endangering the privacy of inner lives, as well as the moral and legal issues surrounding thoughts and actions. Evidence shows that neurotechnologies can alter self-perception, control, and autonomy. Therefore, it is essential to safeguard people’s rights at the cognitive and psychological levels. In a comment published in Nature[28], the same authors expand on this subject,

emphasizing the need for society to return to the bioethical principles of the Belmont Report, namely: justice and equitable access to neurotechnological benefits; the application of the principles of beneficence and non-maleficence to the human mind; and respect for patient autonomy. Beyond these principles, they highlight the need to respect mental privacy, protect neural data, and preserve personal identity and individual agency. The authors argue that the development of neurotechnologies must be guided by proactive ethical and legal frameworks rather than reactive measures. They advocate for regulations that ensure informed consent, data protection, transparency, and fairness in access. Beyond technical safety, they highlight the broader moral responsibility of scientists, policymakers, and society to prevent misuse and inequality. Ultimately, the article proposes that ethical reflection should evolve in parallel with scientific progress, so that innovation in neuroscience and AI promotes human flourishing rather than undermining mental integrity or deepening social divides.

Another article on this subject[29] emphasizes the need for democratic and inclusive global efforts to establish coordinated guidelines for the responsible development of neurotechnologies. It calls for the creation of new protective measures for neural data – so-called “neurorights” – to ensure informed consent, user control, security, and privacy. The authors also recommend developing methods to identify and prevent bias in neurotechnologies, both in their technical design and in their accessibility and use. Finally, they highlight the importance of adopting public policies that guarantee the safe and equitable distribution of these technologies, ensuring that their benefits are broadly accessible to all.

The race to legislate in this area is still in its early stages, but some countries have already taken pioneering and concrete steps. A prime example is Chile, which became the first country to constitutionally recognize neurorights in 2021 through an amendment to Article 19 of its Constitution. Legislative initiatives have subsequently sought to further regulate neurotechnologies, illustrating the evolving nature of this legal framework.

During the ongoing reform of the Brazilian Civil Code, the legislature has proposed to include in the legislation the concept of neurorights, understood as those protections aimed at preserving mental privacy, personal identity, free will, fair access to brain augmentation or improvement, mental integrity, and protection against biases of natural persons, arising from the use of neurotechnologies.

BJP PRE-PROOF

Furthermore, it proposes to guarantee them the same protection as legal personality – the capacity recognized by law for a person to acquire rights and assume obligations – meaning these rights cannot be transferred, waived, or limited. As of the time of writing, this proposal remains under legislative deliberation and has not yet been enacted into law.

Brazil thus finds itself in a transitional moment: while no specific neurorights legislation has been incorporated into the national legal order, the debate is gaining institutional traction, and the existing framework – particularly the LGPD – already offers partial, if incomplete, protection for biometric and neural data. At the subnational level, the State of Rio Grande do Sul amended its Constitution in 2023 to recognize the right to mental integrity; however, given the limited scope of state constitutional provisions within the Brazilian Federal System, this initiative carries minimal practical impact on the broader national legal order.

These developments highlight the growing ethical and legal challenges posed by neurotechnologies and other monitoring systems capable of collecting sensitive physiological or neural data. As such technologies advance and become more integrated into healthcare, concerns regarding mental privacy, data protection, and potential misuse by institutions or third parties become increasingly pressing. The protection of neural and physiological data thus emerges as a critical dimension of patient autonomy and human dignity in the digital health era.

Beyond data protection, the increasing reliance on algorithmic decision-making within IMDs raises concerns about embedded bias and technological paternalism. Algorithms trained on incomplete or non-representative datasets may disproportionately affect vulnerable populations, reinforcing existing inequities in mental health care. Moreover, automated therapeutic interventions may subtly shift clinical authority from shared decision-making toward opaque computational processes, challenging traditional models of psychiatric responsibility and accountability.

For psychiatrists, these challenges are not merely theoretical. They directly affect clinical judgment, capacity assessments, and the therapeutic alliance, particularly when treatment refusal, relapse, or cognitive fluctuation are involved.

In conclusion, while the IMDs represent a technological advancement in healthcare, their implementation will depend on overcoming complex obstacles that extend beyond engineering. Issues of patient autonomy, ongoing consent, data

BJP PRE-PROOF

privacy, and the logistics of long-term treatment for a vulnerable population require equally innovative solutions. Therefore, the future of implantable technologies must be guided by a robust, patient-centered ethical-legal framework that ensures the pursuit of safety does not compromise the dignity, self-determination, and rights of those most in need of protection.

Conflicts of interest

The authors declare that they have no financial, commercial, political, academic, or personal conflicts of interest related to this manuscript within the past three years. The authors further affirm that there are no conflicts of interest relevant to the publication of this article. The senior author (TMF) is funded by grant #313241/2022-8, National Council for Scientific and Technological Development (CNPq).

AI disclosure

The figures in this manuscript were created with the assistance of artificial intelligence tools and subsequently reviewed and validated by the authors for accuracy and consistency with the content presented.

Author contributions

FAPM and APSSM were responsible for conceptualization and methodology. FAPM led the literature review, formal analysis, and writing – original draft preparation. APSSM contributed to methodology, critical analysis, and writing – original draft preparation and review & editing. TMF contributed to supervision and writing – review & editing. All authors have read and approved the final version submitted and take public responsibility for all aspects of the work.

Edited by: Thiago Henrique Roza

REFERENCES

1 Jasim M, Al-Gburi AJA, Hanif M, Dayo ZA, Ismail MM, Zakaria Z. An extensive review on implantable antennas for biomedical applications: Health considerations, geometries, fabrication techniques, and challenges. Alexandria Engineering Journal. 2025;112:110–39.

BJP PRE-PROOF

2 Abhinav V, Basu P, Verma SS, Verma J, Das A, Kumari S, et al. Advancements in Wearable and Implantable BioMEMS Devices: Transforming Healthcare Through Technology. Micromachines. 2025;16:522.

3 Figee M, Riva-Posse P, Choi KS, Bederson L, Mayberg HS, Kopell BH. Deep Brain Stimulation for Depression. Neurotherapeutics. 2022;19:1229–45.

4 Denys D, Mantione M, Figee M, van den Munckhof P, Koerselman F, Westenberg H, et al. Deep brain stimulation of the nucleus accumbens for treatment-refractory obsessive-compulsive disorder. Arch Gen Psychiatry. 2010;67:1061–8.

5 Chen D, Zhao Z, Shi J, Li S, Xu X, Wu Z, et al. Harnessing the sensing and stimulation function of deep brain-machine interfaces: a new dawn for overcoming substance use disorders. Transl Psychiatry. 2024;14:440.

6 Austelle CW, O'Leary GH, Thompson S, Gruber E, Kahn A, Manett AJ, et al. A Comprehensive Review of Vagus Nerve Stimulation for Depression. Neuromodulation. 2022;25:309–15.

7 El-Rashidy N, El-Sappagh S, Islam SMR, M. El-Bakry H, Abdelrazek S. Mobile Health in Remote Patient Monitoring for Chronic Diseases: Principles, Trends, and Challenges. Diagnostics (Basel). 2021;11:607.

8 Radhoe SP, Veenis JF, Brugts JJ. Invasive Devices and Sensors for Remote Care of Heart Failure Patients. Sensors (Basel). 2021;21:2014.

9 Mukherjee S, Suleman S, Pilloton R, Narang J, Rani K. State of the Art in Smart Portable, Wearable, Ingestible and Implantable Devices for Health Status Monitoring and Disease Management. Sensors (Basel). 2022;22:4228.

10 Schulz S, Harzheim L, Hübner C, Lorke M, Jünger S, Woopen C. Patient-centered empirical research on ethically relevant psychosocial and cultural aspects of cochlear, glaucoma and cardiovascular implants – a scoping review. BMC Medical Ethics. 2023;24:68.

11 Wang J, Zhang L, Wang X, Dong J, Chen X, Yang S. Application of Nano-Insulin Pump in Children with Diabetic Ketoacidosis. Journal of Nanoscience and Nanotechnology. 2021;21:5051–6.

12 Chan L, Moster MR, Bicket AK, Sheybani A, Sarkisian SR, Samuelson TW, et al. New Devices in Glaucoma. Ophthalmol Ther. 2023;12:2381–95.

13 COHEN IG, GERKE S, KRAMER DB. Ethical and Legal Implications of Remote Monitoring of Medical Devices. Milbank Q. 2020;98:1257–89.

BJP PRE-PROOF

14 Hwang BY, Negoita S, Duy PQ, Tesay Y, Anderson WS. Opioid use and spinal cord stimulation therapy: The long game. Journal of Clinical Neuroscience. 2021;84:50–2.

15 Huang H-W, Chai PR, Lee S, Kerssemakers T, Imani A, Chen J, et al. An implantable system for opioid safety. Device. 2024;2.

16 Volkow ND, Blanco C. The changing opioid crisis: development, challenges and opportunities. Mol Psychiatry. 2021;26:218–33.

17 A. Marco C. Opioid Overdose and Capacity. The American Journal of Bioethics. 2024;24:33–4.

18 Marshall KD, Derse AR, Weiner SG, Joseph JW. Revive and Refuse: Capacity, Autonomy, and Refusal of Care After Opioid Overdose. Am J Bioeth. 2024;24:11–24.

19 Joseph JW, Marshall KD, Reich BE, Boyle KL, Hill KP, Weiner SG, et al. How Emergency Physicians Approach Refusal of Observation after Naloxone Resuscitation. The Journal of Emergency Medicine. 2020;58:148–59.

20 Biernacki K, McLennan SN, Terrett G, Labuschagne I, Rendell PG. Decision-making ability in current and past users of opiates: A meta-analysis. Neuroscience & Biobehavioral Reviews. 2016;71:342–51.

21 Lyzwinski LN, Elgendi M, Menon C. Users' Acceptability and Perceived Efficacy of mHealth for Opioid Use Disorder: Scoping Review. JMIR Mhealth Uhealth. 2024;12:e49751.

22 Tunzi M, Satin DJ, Day PG. The Consent Continuum: A New Model of Consent, Assent, and Nondissent for Primary Care. Hastings Cent Rep. 2021;51:33–40.

23 Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: A comprehensive survey. J Biomed Inform. 2015;55:272–89.

24 Rainey S, McGillivray K, Akintoye S, Fothergill T, Bublitz C, Stahl B. Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology? J Law Biosci. 2020;7:lsaa051.

25 Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. JAMA. 2018;320:231–2.

26 Jain I, Sellers GS, Jain A, Agarwal A, Davé RS. Chapter Three - The ethical and regulatory landscape of wearable, ingestible, and implantable technologies in

BJP PRE-PROOF

the United States. In: Mahato K, Pandya A, editors. Progress in Molecular Biology and Translational Science, vol. 216. Academic Press; 2025. p. 49–85.

27 Goering S, Yuste R. On the Necessity of Ethical Guidelines for Novel Neurotechnologies. Cell. 2016;167:882–5.

28 Yuste R, Goering S, Arcas BA y, Bi G, Carmena JM, Carter A, et al. Four ethical priorities for neurotechnologies and AI. Nature. 2017;551:159–63.

29 Goering S, Klein E, Specker Sullivan L, Wexler A, Agüera y Arcas B, Bi G, et al. Recommendations for Responsible Development and Application of Neurotechnologies. Neuroethics. 2021;14:365–86.

BJP PRE-PROOF