ISSN: 2641-1911

Archives in Neurology & Neuroscience

DOI: 10.33552/ANN.2026.18.000934

Iris Publishers

Review Article

The Inadequacy of Current Regulatory Frameworks for Securing Next-Generation Brain-Computer Interfaces: A Call for Proactive Cybersecurity Integration

Er Kritika*

Independent Researcher (Neuro-Cybersecurity), India

***Corresponding author:** Er. Kritika, Independent Researcher (Neuro-Cybersecurity), India.

Received Date: January 15, 2026

Published Date: January 20, 2026

Abstract

The brain-computer interfaces have reached unprecedented clinical maturity, but the cybersecurity is severely lacking in the regulatory frameworks of neural interfaces. The existing FDA recommendations and European Medical Device Regulation consider BCIs as conventional medical devices and do not acknowledge the characteristic threat environment where the failure to secure compromises a not only ready but also cognitive freedom. The paper argues that the regulatory paradigm is overdue to change its reactive security guidelines to mandatory and enforceable cryptographic defenses and adversarial testing mechanisms. It is based on recent research showing adversarial attacks on neural decoding algorithms and vulnerabilities in commercial BCIs that we suggest a tiered certification system that incorporates security-by-design concepts into premarket approval procedures prior to massive deployment making neural infrastructure un-vulcanisable.

Keywords: Brain-Computer Interface; Neuro-Cybersecurity; Neural data privacy; Cognitive liberty; Neuroethics

Introduction

The Regulatory-Technology Gap

Brain-computer interfaces are no longer an experimental system but an FDA-approved commercial platform capable of restoring communication to those with paralysis and thought-controlled digital communication [1,2]. Although the advances are impressive, the cybersecurity architectures working with such devices are still pegged on the paradigms that were created to work with passive implants instead of networked cognitive interfaces [3]. The most recent changes in the legislation, such as the state of California regarding neural data as sensitive personal information according to the Consumer Privacy Act, indicate the increased awareness of the privacy specificity of the BCIs, but the security of these devices is still not regulated successfully [4].

The FDA guidance on medical devices cybersecurity only offers suggestions but does not include technical standards that are enforced against neural interfaces. The European Medical Device Regulation also touches on the issue of cybersecurity in general strokes without considering the threat model specifics posed by devices capable of decoding and possibly even modulating neural activity. This failure in regulation is a type of category error having the effect that it attempts to in effect classify BCIs as medical devices where they are undergoing safety validation and not cyber-physical systems that require security-first architecture [5]. The paper will focus on the particular drawbacks of existing regulatory strategies, typifies the unique threat environment of neural interfaces according to the recent studies on cybersecurity, and suggests the tangible certification reform suggestions that are based on adversarial threat modelling.

The Unique Threat Landscape of Brain-Computer Interfaces

Neural Data as Unprecedented Privacy Risk

BCIs analyze neural data that demonstrate mental states and emotional tendencies and possibly thoughts that are too secretive to be revealed in conventional biometric data [4]. A study on the use of consumer neurotechnology as an aspect of privacy reported that business organizations seem to be free to access the neural information of the users with little to no restrictions on how the information is used. This provides a kind of surveillance that has never been seen before in medical equipment: unlimited access to the very substance of consciousness. The ethical guidelines that apply to neural data, as formulated by the International Bioethics Committee of UNESCO, highlight mental integrity, personal identity, psychological continuity, autonomy, and mental privacy as key issues [4]. These values go beyond standard bioethics to neuroethics specifically due to the fact that neural information poses a unique threat to cognitive liberty which is the most essential right to freedom of thought and self-determination of mental activity [6].

Adversarial Attacks on Neural Decoding Algorithms

The are now activated by machine learning algorithms that enable neural signals to be interpreted into their desired movements, speech, or mental states. The latest studies have confirmed that such classifiers are susceptible to adversarial machine learning attacks in which well-constructed input signal perturbations lead to a misclassification (Meng et al., 2024) [2]. In contrast to adversarial examples in computer vision, where digital examples need to be manipulated, neural signal perturbations may potentially be instigated by electromagnetic perturbation or damaged electrodes and thus, such attacks are possible in practice when deployed in the real world. Research has revealed that using adversarial perturbations can insert noise on EEG signals to control BCI spellers to print otherwise incorrect characters at will, and a backdoor attack can induce poisoning in training data to cause certain classifications even with incorrect neural data [1]. In the case of clinical BCIs that operate prosthetic limbs, predict seizures or adjust the parameters of brain stimulation, these attacks would pose a direct risk to the safety of the subject using the corrupted motor instructions or unsuitable therapeutic procedures. Researchers in the field of cybersecurity have generated various attack vectors such as adversarial filtering-based evasion attacks, attacks used during training, and universal adversarial perturbations capable of deceiving BCI systems in different users [2]. Such attacks have impact on the underlying machine learning structures on which present-day BCI action can be practically applied, which constitutes vulnerabilities that do not readily resolve by means of conventional medical device safety testing.

Communication Protocol and Physical Layer Vulnerabilities

In addition to algorithmic attacks, BCIs have the standard cybersecurity negative aspect of communication protocols and physical interfaces. Studies have established that consumer EEG hardware sends neural signals through Bluetooth and with minimal encryption, it is possible to eavesdrop brain activity. Medical grade BCIs frequently use proprietary wireless protocols, which lack an adequate level of cryptographic protection, and do not use best practices like authenticated encryption or perfect forward secrecy [3]. Another issue is physical layer attacks. Studies have established that the EEG equipment wires serve as unintentionally antennal and an attacker can inject fake brainwave signal via radio-frequency communication that the amplifier built into the equipment will interpret as a real brainwave. In invasive BCIs that have percutaneous connections, physical access to such interfaces may make it possible to directly manipulate signals, or steal data.

Regulatory Framework Inadequacies

FDA Guidance Limitations

The FDA regulation of BCI adheres to standard medical device procedures and cybersecurity is taken care of by advisory documents that are not mandatory but suggest certain security practices. This system has fatal weaknesses when transferred to neural interfaces. To begin with, the guidance does not set binding technical requirements of cryptographic implementations but only gives guidance, which lets manufacturers assert compliance by documentation but leaves them without the actual deployment of secure encryption protocols. Second, the substantial equivalence pathway does not welcome security innovation because it encourages manufacturers to show that proposed new BCIs are functionally identical to the security architecture of existing devices instead of providing enhanced security. Third, the post-market surveillance systems are based on the principle of adverse events reporting, which are incapable of identifying advanced cyberattacks that would not be prominent but instead are expressed in the form of slow performance loss. The sad part is cybersecurity review does not have special knowledge in the fields of neurotechnology and security threat modeling. Bioengineered reviewers might not be aware of advanced attack vectors that are specific to neural decoding algorithms or not perceive the special privacy concerns of exfiltration of neural data [3].

European MDR Shortcomings

European Medical device regulation mandates manufacturers to deal with risks posed by cybersecurity attacks but does not impose any technical standards of BCI, no compulsory adversarial testing or specialized review of devices that process neural data.

The very procedure of CE marking is based on the Notified Bodies which in most cases do not have profound knowledge in the field of neurotechnology and cybersecurity, which leads to knowledge gaps in conformity assessment.

Consumer Neurotechnology Regulatory Vacuum

The most obvious deficiency is, perhaps, the fact that consumer neurotechnology devices have nearly no control over them. EEG headsets being sold as meditation, playing games or cognitive training are not subject to FDA or MDR regulation, but retrieve neural information that indicates sensitive cognition. This establishes a two-level framework in which therapeutic BCIs barely undergo any scrutiny of their security and consumer appliances having up to millions of users move on practically without any binding security regulation.

Toward Proactive Cybersecurity Integration

Core Principles for BCI Security Regulation

A sufficient regulatory framework should be based on the principles of security-by-design where cybersecurity requirements will be considered at the earliest design phases as opposed to being added at the end to meet the compliance demands. This framework needs to assume motivated, advanced adversaries by carrying out formal threat modeling under the documents of listing attack vectors and certifying defenses by conducting penetration testing. To implement BCI, there is a need to have a series of layered defenses that move through a physical security attack, cryptographic protection, secure communications, protection based on algorithmic robustness against adversarial or malicious ways of an attack, and also safe use of software engineering [3]. In contrast to the previous condition of medical devices where encryption can be regarded as an option, modern BCIs cannot and should use cryptographic protection because of the available low-power implementation.

Tiered Certification Framework

A hierarchical certification scheme which fits neural interfaces is suggested as below:

Tier 1 - Foundational Security (All BCIs): all interfaces between brains and computers (including consumer devices) should be acting across approved cryptographic algorithms in either way, ensure secure booting so as to prohibit unreputable firmware modification, require access control, which implements principle of least privilege, secure firmware update with cryptographic signature verification and mandatory vulnerability disclosure programs with predefined response times.

Tier 2 - Enhanced Protection (Medical-Grade BCIs): Therapeutic device requirement devices should also show formal threat models documentation, independent security researcher penetration tests, hardware security modules to store cryptographic keys, data integrity safeguards to prevent the unauthorized modification of neural records or stimulation settings, and adversarial solidity tests to machine learning classifiers of conventional attack vectors [2].

Tier 3 - High Assurance (Implantable BCIs): Invasive neural interfaces should include the utmost requirements such as formal verification of critical security properties, Byzantine fault tolerance of control algorithms, hardware attestation to verify the integrity of remote device, and neural data processing with differential privacy.

Neural Data Protection Standards

In addition to security measures of devices, the regulatory frameworks should also cover the privacy implications of neural information that are unique, and require the introduction of data minimization principles in a mandatory way. BCIs must also process only the amount of neural data needed to perform the desired function, and these controls must be strict on retention and second usage [4]. Neural data must be treated as an exclusive level of sensitive personal data that has to be given a more aggressive protection and take the example of the California legislation. Raw neural recordings are to be considered as sensitive with edge processing being preferred to extract the needed features and remove raw signals. In case of the need to perform central processing, the use of techniques of differential privacy should be used to ensure that no unintended information is re-identified and inferred.

Addressing Implementation Challenges

The industry stakeholders will object on the basis of cost, development schedule, and tradeoff on performance. But these arguments cannot explain the much higher costs of patient and manufacturer security breaches in form of liability damages, recalls, and reputation damages. Additionally, security integration at the early stage is incredibly cheaper than security retrofitting on devices that are already deployed [3]. Contemporary low-power cryptographic designs are small performance wise such that security overheads are insignificant when compared to signal processing overheads required by invasive BCIs as well as completely manageable when using commercial processors on consumer devices. There is no need to lock down security to avoid emergency access; cryptographic mechanisms can offer authorized emergency override mechanisms just as is the case in other systems with high security requirements. The supposed fear that tough requirements will suppress innovation flips the real relationship clear security requirements decrease uncertainty, eliminate the need to patch applications after the fact, and make the security system trusted by the general populace to be adopted pervasively. The other option which is the use of insecure devices that are highly vulnerable to attacks will cause way more harm to neurotechnology sector than active security demands.

Conclusion

The insufficiency of existing regulatory framework to BCI cybersecurity is posing a risk to patient safety, privacy and cognitive liberty with neural interfaces progressing between experimental to mainstream medical devices and products consumed by the population. We have studied the experience of cardiac device security failures that voluntary guidelines and responsive actions are inadequate. The special threat environment of BCIs, encompassing adversarial schemes against neural decoding algorithms, communication protocols exposure, and never-before-seen risks of neural data privacy, necessitate radically different regulatory frameworks based on compulsory cryptography, adversarial tests, and security of the lifecycle. The tiered certification structure suggested by us offers a good implementation direction, as it offers security requirements and device capabilities and offers the most important devices the highest protection levels. The peculiarities of the differences between BCIs and common medical devices are covered with specialized review procedures including cybersecurity skills and neural data protection requirements. The well-being of the single device is not only personal but also that of human-computer interaction in the neural level in the future. Unless we put in place strong security bases today, we are facing a future where even the most personal areas of human cognition will be susceptible to surveillance, manipulation and control.

Acknowledgement

None.

Conflict of Interest

No Conflict of interest.

References

1. Kumar N, Deshkar D, De S, Saini A, Kania RP, et al. (2025) A comprehensive analysis of security flaws and attack vectors in artificial intelligence-powered brain-computer interfaces. Vascular and Endovascular Review 8(6s): 106-121.
2. Meng L, Jiang X, Chen X, Liu W, Luo H, et al. (2024) Adversarial filtering-based evasion and backdoor attacks to EEG-based brain-computer interfaces. IEEE Transactions on Information Forensics and Security 19: 1-15.
3. Schroder T, Sirb R, Par S, Morle J, Stree S, et al. (2025) Cyber risks to next-gen brain-computer interfaces: Analysis and recommendations. Neuroethics 18: 34.
4. Yang H, Jiang L (2025) Regulating neural data processing in the age of BCIs: Ethical concerns and legal approaches. Digital Health 11: 20552076251326123.
5. Kritika E (2025) Ethical Frontiers: Navigating the Intersection of Neurotechnology and Cybersecurity. Journal of Experimental Neurology 6(1): 21-25.
6. Kritika EM (2024) Neuroethical quandaries at the crossroads of cyberspace. Scientific Practical Cyber Secur J.