NOVA Policy Network
Policy Brief

Are Existing Data Privacy Laws Sufficient for Neural Data?

HIPAA / Neurodata

<Murari Ambati>

Policy Brief

Date, December, 23, 2024

Executive Summary

As neurotechnology is advancing speedily, the collection and use of neural data like brainwave patterns, signals from implants, and other neurological biomarkers raise new challenges for the conventional data privacy and protection regimes. The Health Insurance Portability and Accountability Act (HIPPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union were enacted primarily to safeguard traditional health and personal information. But neural information is fundamentally distinct in its sensitivity, susceptibility to abuse, and impact on individual autonomy and psychological privacy.

Current legal regimes do not quite capture neural data as a specific category which requires to be given greater protection, and therefore there is significant legal uncertainty over consent, ownership of data, and permitted uses. In addition, new neurodevices can acquire very grained brain activity at all times and make unprecedented inferences about thoughts, intentions, and emotional states. This observation blurs the adequacy of current regulation based on informed consent and data minimization since neural data may reveal very intimate information even after de-identification.

This summary examines the loopholes in HIPAA and GDPR when it comes to neurodata's special threats, including unclear coverage of implant data, insufficient standards for de-identification of cognitive data, and the necessity of provisions for mental privacy comparable to physical privacy protections. It takes into account increasing commercial and research applications of neurodata as well as cross-border data flows that complicate enforcement. Lastly, the brief argues on behalf of the development of specialized neurodata privacy law or amendments to existing legislation that recognize the distinct nature of neural data and offer robust protections that evolve with technological development.

Introduction

The advent of neurotechnology has introduced a new type of personal data: neural data—high-definition data derived from the electrical activity, shape, or function of the brain. As more advanced devices such as brain-computer interfaces (BCIs), EEG headsets, deep brain stimulators, and implantable neuroprosthetics become available, they generate streams of data exponentially more extensive than traditional medical records. The neural data can include raw recordings of brainwaves, inferred emotions, thought patterns, intentions, or even memory-associated signals. The ability to harvest, store, and decode such personal data bewilders the foundational assumptions of the existing data protection law.

In the US, HIPAA governs covered entities' privacy and security of PHI in health care and insurance organizations. HIPAA, however, only covers covered entities and their affiliates—not most consumer neurotech companies, wellness platforms, or even some research scholars. Consequently, EEG data collected by a mobile neurofeedback system or brain activity extracted by a brain-training software might not qualify as PHI and thus may be gathered, sold, or reused without significant consent or control.

In the EU, GDPR is even more comprehensive in characterizing biometric and health information as sensitive categories that must be under stricter controls. But like the HIPAA Rule, it is also mum about neurodata and does not yet anticipate the inferential damages that accompany brain-derived information. GDPR's focus on ”personal data” does not address questions regarding inferred mental state and patterns of thought, particularly in de-identified or pseudonymized information that would nevertheless carry cognitive fingerprints.

Furthermore, neither HIPAA nor GDPR entirely foresees the new issues of cognitive freedom, neuroprivacy, and mental sovereignty—presuming an individual can maintain his or her brain-derived information and thought processes fully in control. With improving neural signal-reading AI algorithms, mental surveillance and decoding without permission pose a growing risk. Without changing regulation, the most private aspects of our minds might become commercially or even politically exploitable.

This paper seeks to evaluate whether HIPAA and GDPR, as they stand and are being implemented, can effectively govern the collection, processing, and sharing of neurodata. It documents inherent legal and conceptual limitations in both approaches and presents pathways to a rights-oriented, future-proof approach to protection of neural information in the face of rapid advances in neurotechnology.

Issues / Policy Gaps

Neural data occupies a legal and moral grey zone under existing data privacy laws. While HIPAA and GDPR provide the building blocks for safeguards over traditional health and biometric information, these were not designed to address the new risks associated with brain-derived data. Therefore, there are relevant gaps in policy along multiple axes of neurodata governance, from classification in the law and consent processes to reuse of data, inference risk, and transboundary transport.

Arguably the most urgent is the scope of HIPAA jurisdiction. The law applies only to "covered entities" such as hospitals, healthcare providers, and insurance firms, and their business associates. Few neurotechnology creators, particularly those involved in consumer wellness or performance enhancement, fall into these groups. Hardware that tracks brainwave activity, levels of attention, or mood signals for non-medical purposes can collect highly sensitive cognitive data without being required to abide by HIPAA's privacy and security rules. This establishes a dual system where medical neurodata is protected but commercial neurodata is largely unregulated.

Second, neither HIPAA nor GDPR has a clear legal definition of neural data. While GDPR does extend to health data and biometric data as part of "special categories," it does not specifically mention EEG signals, brain-computer interface information, or other premium neurotechnology outputs. More basically, GDPR's formulation addresses "identifiable" information, while neural signals—although seeming to be anonymized—often can be reversed-engineered to reveal personality traits, emotional conditions, or mental illness. This undermines inferences about inference-based reidentification risk security over de-identified data and reveals a central failure of inference-based reidentification risk.

Third, existing models lack clearly defined data ownership and access rights for subjects over their neural data. While GDPR guarantees data access, correction, and portability, these are difficult to exercise in real-time, high-frequency brain implant or BCI headset data. Neural data is also hard to contextualize; while a reading of blood pressure is easily convertible to one quantitative value, neural data might not be so convertible to one quantitative value. Without ownership norms or cognitive data standards, users are usually uncertain what they are consenting to, or how their mental signals can be reused or resold.

Fourth, there are inadequate procedures concerning informed consent when it comes to the collection and secondary use of neural data. Traditional consent models have developed approaches to explicit agreement at the time of data collection but do not respect the complexity of later uses such as behavioral profiling, training AI, or predictive analytics. Neural data is highly fluid and may be interpreted in a manner never considered at the outset. Thus, current forms of consent might satisfy the letter of the law but are ethically inept.

Finally, both HIPAA and GDPR are not geared to handle cross-border neurodata flows and the challenges of global regulation. Neurodevices are now being retailed globally through digital platforms, so data may be stored in one country, processed in another, and analyzed in a third. Without a coordinated regime of neurodata regulation, enforcement becomes difficult and there are loopholes for business players to exploit gaps in regulation.

Such policy loopholes demonstrate that HIPAA and GDPR, as they exist today, cannot safeguard the ethical, legal, and psychological dimensions of neural data. The current protections need to be supplemented by a new generation of safeguards uniquely tailored for neurodata to maintain individual autonomy, prevent cognitive exploitation, and foster public trust in the future generation of brain-based technologies.

Policy Recommendations

In order to guarantee that neural data is handled with the care and safeguard it deserves, policymakers need to take the lead in creating a specific regulatory framework that transcends the limitations of HIPAA and GDPR. This starts by officially classifying neural data as a unique and high-risk type of personal information. In contrast to traditional biometric data, neural data have the ability to inform not just of a person's physical or behavioral characteristics, but of their mental states, intentions, moods, and even memories. The law should thus be observed to be attuned to this greater sensitivity through enacting separate legal definitions and coverages relevant to the nature of brain-derived information.

Regulators are also required to introduce a tiered approach to regulation based on the context under which neurodata is collected and the threat that poses to individuals' autonomy. Wellness apps' non-intrusive brainwave scans, for instance, may require only moderate measures of protection, while invasive data extracted from neural implants or used in predictive behavioral profiling must elicit stricter standards of disclosure, ethical scrutiny, and minimization of data. The model comes with flexibility but has proportionate measures of protection.

The other significant recommendation is to reform current practices of consent. The collected neural data for consent must be dynamic, contextual, and continuous. Users should not only be informed of the collection and storage of their neurodata but also about potential future uses and inferences that may arise in the future due to changing algorithms. Opt-outs and live consent dashboards should be made uniform across all commercial neurotech devices, as well as secondary use bans with explicit permission. This will return agency to a field where user consciousness falls behind technical skill.

Also essential is the requirement for a centralised regulatory body empowered to certify, watch, and audit neurotechnology platforms. This body—if established as a novel federal commission or as a special unit of one—is to possess standards jurisdiction over neurodata, mandate risk reporting, and collaborate with global partners to monitor cross-border data flows. In addition, the entity should establish standards of ethical AI models derived from brain data and punish misuse or unauthorised inference.

Finally, policy has to codify a new range of cognitive rights that protect individuals from excessive interference, manipulation, or commercialization of their mental states. These rights would legitimize the individual's control over his/her brain data, permit access and delete rights, and ban surveillance or profiling activities based on cognitive inference. By enacting such rights into law, governments can ensure that neurotechnology advances under a human-centered, rights-based regime rather than an exclusive commercial regime.

Collectively, these proposals make up a vision for an anticipatory, ethical, and resilient framework of governance for neurodata. With the brain ushering in the future of data gathering, systems of governance must respond to the challenge—to ensure the inner life of the mind is protected in an increasingly connected world.

Conclusion

As neurotechnology moves from idea to consumer product and clinical use, personal data protection regimes must catch up. Neural data is not merely a type of health data—it is a new type of intimate, inferentially dense, and psychologically charged data that such schemes as HIPAA and GDPR were never designed to regulate in its entirety. While these statutes offer some protection, they do not have the definitional precision, enforcement provisions, and conceptual sophistication necessary to reach all of the risks posed by brain-derived information.

This briefing has revealed that existing regulatory status quo renders neural data extremely vulnerable. Commercial uses of neurotech are outside the scope of HIPAA, and GDPR fails to appropriately account for inferential strength or identity risk present in cognitive signals. Issues around consent, ownership, inference risk, and cross-border regulation remain unresolved. Without intervention, there is growing potential for cognitive surveillance, abuse of data, and erosion of mental privacy.

To maintain trust and respect in the neurotechnology era, policy has to keep pace with science. Tools provide a rational means to sort and control varied neural data uses according to their true harm potential. Cognitive rights protection and even novel regulation agencies through legal reform have to be active, dynamic, and based on a moral system that regards the mind as sacrosanct.

Ultimately, governance of neurodata is not merely a data problem but a problem of human freedom. Protecting thought, emotion, and intention from commodification or surveillance is a quintessential challenge of the 21st century—and one that requires urgent and concerted policy action across national and disciplinary boundaries

References

1. Greely H, Sahakian B, Harris J, Kessler RC, Gazzaniga M, Campbell P, Farah MJ. Towards responsible use of cognitive-enhancing drugs by the healthy. Nature. 2008 Dec 11;456(7223):702-5. doi: 10.1038/456702a. Erratum in: Nature. 2008 Dec 18;456(7224):872. PMID: 19060880.

2. Ienca, M., Andorno, R. Towards new human rights in the age of neuroscience and neurotechnology. *Life Sci Soc Policy* 13, 5 (2017). https://doi.org/10.1186/s40504-017-0050-1

3. Presidential Commission for the Study of Bioethical Issues. (2014). *Gray Matters: Topics at the Intersection of Neuroscience, Ethics, and Society*. Washington, D.C.

4.. Sandra Wachter, Brent Mittelstadt, Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Volume 7, Issue 2, May 2017, Pages 76–99, https://doi.org/10.1093/idpl/ipx005

5. European Data Protection Board (EDPB). (2021). *Guidelines 3/2019 on processing of personal data through video devices.*

6. Rocher, L., Hendrickx, J.M. & de Montjoye, YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* 10, 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3