2026 NEURAL DATA COMPLIANCE GUIDE FOR BCI MANUFACTURERS

Data governance, liability, and consent for brain-computer interface manufacturers

FISE Technologies

August 2026

Authored by M.E. Nara Lau, CEO Founder
nara@fise.tech

1. Introduction

Neural and electroencephalogram (EEG) data now occupies a regulatory space that did not exist a decade ago. The highly sensitive nature of brain data stands at the edge of health and biometric data laws which raises new data consent questions. For brain-computer interface (BCI) manufacturers, this creates growing business risks such as overlapping legal jurisdictions, unresolved liability questions, and scarce guidance on how to build compliant infrastructure. In this moment of rapid innovation, most companies are in early-stage development and neglect to address these business risks due to a lack of legal or compliance resources.

This guide can help clarify growing business risks, liability questions, and compare options for compliant infrastructure to help build awareness and navigate the 2026 regulatory landscape for neural data. It reviews regulations that apply to neural data today, the technical standards emerging around BCI data formats and interoperability, and the practical build-versus-buy decision manufacturers face when deciding how to handle consent, identity, and data governance for their products.

As this is not legal advice, it is highly recommended to have this guidance reviewed by qualified counsel who are familiar with manufacturer-specific products, jurisdictions, and data flows. This information provides initial context as a primer to facilitate a clear understanding of these risks and ask the right questions before they are asked by a regulator, data breach investigator, or plaintiff's attorney.

2. Consumer BCI Neural Data and Health Data

Neural data from consumer-marketed BCI products is often not regulated in the same way as clinical health data covered by HIPAA, particularly where the provider is not a HIPAA covered entity or business associate. Neural data also does not map neatly onto traditional biometric categories such as fingerprints or face scans. EEG signals may enable inferences about cognitive and emotional states, raising different and potentially heightened mental-privacy concerns beyond those associated with externally observable physical identifiers.[1]

Regulators and privacy advocates have begun sounding the alarm. In 2024, Colorado and California became the first states to expressly add neural data to their privacy-law frameworks, treating it as a distinct sensitive data category. Connecticut and Montana followed in 2025. Connecticut added neural data to its definition of sensitive data, with the provision taking effect July 1, 2026, while Montana enacted what has been described as the most detailed existing state consent framework

1 UNESCO, Recommendation on the Ethics of Neurotechnology, https://www.unesco.org/en/legal-affairs/recommendation-ethics-neurotechnology

for "neurotechnology data." In the first six weeks of 2026, nine neurodata related bills were introduced across six states.[2]

Investors evaluating BCI companies can reasonably be expected to scrutinize data governance and neuro privacy more closely during due diligence, given that consent architecture directly affects regulatory exposure under emerging state neural data regimes. Cyber insurance underwriters, who already evaluate data breach and sensitive data risk more broadly, may extend similar scrutiny to neural data consent and access controls as claims and enforcement activity develop. As BCI manufacturers move toward original equipment manufacturer (OEM) licensing and platform partnerships, enterprise buyers may also face potential downstream liability, contractual, and compliance risks under applicable state privacy laws. Manufacturers therefore have a strong incentive to treat data governance as a contractual requirement rather than a nice-to-have.[3]

3. Regulatory Landscape

3.1 Biometric Privacy Laws

Illinois's Biometric Information Privacy Act (BIPA) remains the most litigated example of a state biometric privacy law and has produced substantial settlements against companies who were alleged to have collected biometric identifiers without the written notice and release required by BIPA. Other states have enacted biometric privacy statutes that commonly impose notice and consent requirements. In some jurisdictions, obligations extend to retention, destruction, or security enforcements which may be governmental, private, or both. Whether a given jurisdiction's biometric statute reaches EEG or neural signal data is often unsettled and should be assessed with counsel on a state-by-state basis rather than assumed.[4]

3.2 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies to protected health information handled by covered entities and their business associates, including healthcare providers, health plans, healthcare clearinghouses, and vendors that handle PHI on their behalf. Most consumer BCI products fall outside this framework when their manufacturers are not HIPAA covered entities or business associates. However, if a consumer-oriented manufacturer later provides services for a covered entity and, in doing so, creates, receives,

2 Arnold & Porter, Neural Data Privacy Regulation: What Laws Exist and What Is Anticipated? https://www.arnoldporter.com/en/perspectives/advisories/2025/07/neural-data-privacy-regulation

3 KFF Health News, States Pass Privacy Laws To Protect Brain Data Collected by Devices, https://kffhealthnews.org/mental-health/colorado-california-montana-states-neural-data-privacy-laws-neurorights/

4 Wilmer Hale, Biometric Privacy Law Update, https://www.wilmerhale.com/en/insights/client-alerts/20230224-biometric-privacy-law-update

maintains, or transmits PHI on that entity's behalf, it may become a HIPAA business associate despite its original consumer-directed wearables marketing.[5]

3.3 General Data Protection Regulation (GDPR) & EU AI Act

For manufacturers targeting EU users, the GDPR distinguishes between data controller and data processor. A data controller determines the purposes and essential means of processing and bears primary responsibility for GDPR compliance. A data processor processes personal data based on the controller's documented instructions and carries separately defined statutory obligations. The manufacturer may function as one or both roles, depending on information such as data uses, consent flows, retention, recipients, and access. Section 7 of this guide provides more analysis on GDPR and neural data.[6]

3.4 Emerging Neural Data Laws

Colorado and California have amended their privacy statutes to uniquely address neural data as a distinct category of sensitive data, giving consumers heightened rights over how that data is collected, used, and shared. Colorado requires affirmative opt-in consent to process neural data, while California classifies neural data as sensitive personal information and gives consumers rights to access, correct, delete, and limit certain uses and disclosures.[7]

Although these laws and bills are not fully established due to lack of neural-data-specific enforcement or litigation, privacy litigation precedents could point to biometric and health data laws which have long underscored the dangers of exposure arising from mishandling sensitive data. Neural-data-specific laws are a clear indication that lawmakers view neural data as warranting unique regulatory treatment, rather than assuming the sufficiency of existing regulatory guidance pertaining to biometric or health data categories.[8]

---

5 U.S. Department of Health & Human Services, Covered Entities and Business Associates, https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

6 European Data Protection Board, Data Controller or Data Processor, https://www.edpb.europa.eu/sme/learn-the-basics/data-controller-or-data-processor_en

7 Hunton, Colorado Amends Privacy Act with H.B. 1058, Adding New Protections for Biological and Neural Data, https://www.hunton.com/privacy-and-cybersecurity-law-blog/colorado-amends-privacy-act-with-h-b-1058-adding-new-protections-for-biological-and-neural-data
Baker Botts, California Extends Privacy Law to Cover Neural Data, https://ourtake.bakerbotts.com/post/102jkp7/california-extends-privacy-law-to-cover-neural-data

8 Arnold & Porter, Neural Data Privacy Regulation: What Laws Exist and What Is Anticipated? https://www.arnoldporter.com/en/perspectives/advisories/2025/07/neural-data-privacy-regulation

3.5 Jurisdiction & Laws by Product Type

Product Type	Jurisdiction & Laws	Criteria	Scope
Wearables	State biometric privacy laws, CA & CO neural data rules	Sharing or collecting neural/EEG data	Sharing, consent, retention, deletion
Research or clinical device	HIPAA if covered entity or business associated, research rules, state law	Handling or exposing PHI for a healthcare entity or covered study	PHI, research authorization
OEM	Applicable laws extend across partners	Partners can access, transfer, or use independently	Roles, onward use, contract terms
Marketed to EU	GDPR, EU AI Act	Behavioral monitoring, covered AI use	Controller/processor, transfer, AI classification

4. Current Areas of Manufacturer Liability

Consumer BCI companies have often relied on broad click-through terms and privacy policy acceptance at setup, paired with encryption and de-identification measures for stored data. These are reasonable baseline safeguards, but they may be insufficient on their own under newer neural-data-specific regimes that require per event or per-recipient consent per specified use or downstream transfers to other parties.

- A one-time, broad EULA may not satisfy consent standards increasingly reflected in privacy law, which require consent to be affirmative, specific, informed, and revocable for defined processing purposes. For neural data, Minnesota's proposed SF 1240 would require separate consent for each use and third-party disclosure at each BCI connection.[9]
- De-identification of neural data does not necessarily eliminate anonymity or privacy risks for the subject. Due to unique statistical signatures that can persist across neural data records, "brainprints" in neural signals and EEG patterns may link records to the same individual. An organization should not assume that removing names establishes anonymity. Given increasing

9 State of MN, S.F. 1240, https://www.revisor.mn.gov/bills/94/2025/0/SF/1240/versions/latest/pdf/

scrutiny of biometric data practices, regulators may question whether residual data even if anonymized can reasonably be linked to a device, datasets, or a person.[10]

- Encryption protects data in transit and at rest, but encryption does not determine who is authorized to access it, for what purpose, and the length of time allowable for access. Current privacy laws generate such questions for companies and innovators to address. [11]

As manufacturers move toward OEM licensing and platform partnerships, further complications emerge. Each new partner that accesses the underlying data stream can introduce additional data handling terms, consent considerations, and questions about legal responsibility if something goes wrong. Absent a shared governance framework, the required contractual controls, role allocations, and consent implementation may need to be addressed separately for each partner. This approach can become more costly and legally fragile as the partner network grows.[12]

5. Applicable Technical Standards

In parallel to the evolving legal landscape, technical standards have emerged for how BCI data is structured, stored, and exchanged. While these standards do not resolve prior compliance and liability gaps, they shape how manufacturers can design their products based on approved standards. These technical standards, when implemented, form an interoperable foundation for future compliance solutions that address regulatory and legal risks for BCI manufacturers.

5.1 ISO/IEC TS 27571:2026

This technical specification defines a standardized data format for non-invasive BCI data, including EEG. It specifies basic data elements, technology-specific information, metadata and annotations, an extensible modular structure, and file naming conventions. The standard describes organizing data by subject and session, separating raw data, processed data, and metadata/annotation information.

This structure has implications beyond formatting. It can support an architecture where identity, consent, provenance, and processing history are maintained with metadata and processed data layers, rather than embedded in or continuously modifying the raw real-time signal path. Its modular structure can make a governance layer technically feasible in an existing BCI pipeline, encompassing

10 Scientific Reports, Person-identifying brainprints are stably embedded in EEG mindprints, https://www.nature.com/articles/s41598-022-21384-0

11 Journal of AHIMA (American Health Information Management Association), Encryption Basics, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=908084

12 Risk Management Magazine, Understanding the New Colorado Privacy Act, https://www.rmmagazine.com/articles/article/2021/08/02/understanding-the-new-colorado-privacy-act
European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://www.edpb.europa.eu/system/files_en?file=consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

the end-to-end workflow a BCI product uses to turn neural data into a device action or software output.[13]

5.2 IEEE P2731, P2794, and IEEE/UL 2933 (TIPPSS)

IEEE P2731 helps unify terminology for brain-computer interfaces, supporting clearer messaging and interoperability across BCI systems. IEEE P2794 improves the transparency, interpretability, reproducibility, and comparability of published research by establishing reporting standards for in vivo neural interface research.[14]

IEEE/UL 2933-2024 defines the TIPPSS framework: Trust, Identity, Privacy, Protection, Safety, and Security for clinical internet of things (IoT) data and device interoperability. Although designed for clinical IoT, including wearable and healthcare-connected devices, it provides a useful conceptual framework for brain-machine-interface manufacturers assessing data governance, identity and access, privacy, security, safety, and interoperability across device and platform ecosystems.[15]

5.3 The Gap Between Data and Identity Standards

> *As of this writing, the published scopes of BCI data-format and interoperability standards, such as ISO/IEC TS 27571 and IEEE P2731/P2794, do not specify an integration with identity and consent technologies such as W3C Decentralized Identifiers (DIDs) or Verifiable Credentials (VCs). The BCI standards focus on data structure, terminology, metadata, and research reporting, while DID and VC specifications provide general-purpose frameworks for decentralized identity and cryptographically verifiable claims. Paths for these two standards, BCI data and identity/consent, appear to have developed independently.*

This is a significant gap in the current standards landscape. No identified published standard provides an end-to-end, off-the-shelf framework linking BCI data structure and interoperability to portable identity, purpose-specific consent, access authorization, and auditable proof of data use. ISO/IEC TS 27571 standardizes non-invasive BCI data elements, metadata, and file structure, and does not prescribe a governance layer.

Therefore, manufacturers need to assemble their own governance solutions from multiple legal requirements, technical standards, and contractual controls. Without a common cross-industry

---

13 Swedish Institute for Standards, Information technology — Brain-computer interfaces — Data format for noninvasive brain information collection, https://www.sis.se/en/produkter/information-technology-office-machines/general/isoiec-ts-275712026/

14 IEEE SA, IEEE Draft Trial-Use Standard for Reporting Standards for in vivo Neural Interface Research (RSNIR), https://standards.ieee.org/ieee/2794/11108/

15 IEEE SA, IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS--Trust, Identity, Privacy, Protection, Safety, and Security, https://standards.ieee.org/ieee/2933/7592/

framework, implementations may vary substantially, making interoperability, auditability, and defensibility more difficult.[16]

6. Choosing Between Building and Buying

Once a manufacturer recognizes that EULA + anonymization is not a durable long-term approach, the practical question is how to build a stronger governance model and whether to develop it in-house or adopt a shared, audited infrastructure layer.

6.1 In-House Development: Cost and Complexity

- Engineering and operations:
    1. Designing and maintaining consent, identity, access-control, security, and audit capabilities is an ongoing investment, not a one-time build.
    2. Privacy governance requires continuous monitoring, review, and adjustment as data uses, systems, and risks change.[17]
- Legal and compliance:
    1. Compliance requires continuing jurisdictional analysis, documentation, and updates as legal requirements, product functions, and processing arrangements evolve.
    2. This is especially relevant for neural data, where state laws and proposed bills are developing quickly.[18]
- Independent assurance:
    1. Investing in external audits, assessments, certifications, or other independent assurance may strengthen the credibility of external compliance representations beyond self-attestation.
    2. The assurance mechanism would assess whether data-governance claims comply with applicable legal requirements, customer requirements, and contractual obligations.
- Breach and misuse exposure:
    1. If a manufacturer determines the purposes and means of in-house data processing, the manufacturer will be primarily accountable as the data controller.

16 NIH National Library of Medicine, Towards an understanding of global brain data governance: ethical positions that underpin global brain data governance discourse, https://pmc.ncbi.nlm.nih.gov/articles/PMC10665841/

17 NIST Privacy Framework: A tool for improving privacy through enterprise risk management, https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

18 European Data Protection Board, Data Controller or Data Processor, https://www.edpb.europa.eu/sme/learn-the-basics/data-controller-or-data-processor_en

2. Outsourcing data governance functions to a processor or vendor does not eliminate the manufacturer's responsibility for data governance. Depending on applicable law and the parties' contractual terms, risk and liability may be allocated among the manufacturer, processor, and vendor, including through indemnities and other contractual remedies.[19]

6.2 The Value of Shared, Auditable Infrastructure

A specialized, independently assessed governance layer can reduce duplicated engineering and promote standardized identity, consent, access-control, and audit practices across products and partners. It does not transfer the manufacturer's compliance responsibility. Nevertheless, if properly vetted, contracted, and monitored, it can reduce implementation burden and improve proof of compliance through auditability.[20]

6.3 Actionable Framework

- Map applicable regimes
    1. Identify every privacy, biometric, health, research, and AI regime that applies to the product today and those likely to apply as the roadmap moves into clinical use, EU markets, OEM licensing, or broader data sharing.
    2. A data inventory and processing map are foundational privacy-risk-management practices.[21]
- Test consent design
    1. Assess the current consent mechanism against the consent, disclosure, access, deletion, and revocation obligations in each applicable jurisdiction.
    2. Recent neural data laws increasingly require express consent for sensitive data processing.
    3. Montana requires separate express consent for specified third-party transfers and a mechanism to revoke consent.[22]
- Map partners and data flows

---

19 Covington, GDPR Contracts and Liabilities Between Controllers and Processors, https://www.insideprivacy.com/international/united-kingdom/gdpr-contracts-and-liabilities-between-controllers-and-processors/

20 European Data Protection Board, EDPB adopts Opinion on processors, Guidelines on legitimate interest, Statement on draft regulation for GDPR enforcement, and work programme 2024-2025, https://www.edpb.europa.eu/news/edpb-adopts-opinion-on-processors-guidelines-on-legitimate-interest-statement-on-draft_en

21 NIST Privacy Framework: A tool for improving privacy through enterprise risk management, https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

22 Cooley, Montana on the Brain: A Bold Step for Neural Privacy, https://www.cooley.com/news/insight/2025/2025-04-22-montana-on-the-brain-a-bold-step-for-neural-privacy

1. Identify every current and planned OEM, platform, cloud, analytics, and research partner; document what data each may access, receive, retain, or independently use.
2. Determine whether governance controls and contractual terms apply consistently across the chain.
3. Privacy frameworks emphasize maintaining an inventory of third parties and the data they may access.[23]

- Compare implementation models
    1. Estimate the ongoing engineering, legal, operations, assurance, integration, and vendor-management costs of building in-house versus adopting a specialized external layer.
    2. Estimate the ongoing costs of maintaining governance capabilities in-house versus adopting a specialized external layer.
- Validate role and liability posture
    1. Obtain counsel's assessment of each party's controller, joint-controller, processor, service-provider, or business-associate status.
    2. This analysis depends on the actual allocation of decision-making, particularly who determines the purposes and essential means of processing.[24]

7. Data Management and Liability

Under the GDPR, singular or partnered entities who determine the purposes and essential means of processing personal data are considered the data controller (controller). The data controller carries the primary accountability burden for the processing. An entity that processes personal data on the controller's behalf, and only on the controller's documented instructions except where law requires otherwise, is a data processor (processor). Although this is a different role, processors retain independent GDPR obligations and may face direct regulatory exposure or liability, particularly if they exceed lawful instructions or determine their own purposes and essential means. The classifications of controller and processor depend on the parties' actual activities in the specific processing arrangement. [25]

How a manufacturer designs consent, permissions, and data access can be relevant to its controller–processor classification, but the classification depends on the manufacturer's actual role in each

23 HSFKramer, EDPB Opinion: How far down the supply chain do controller duties extend? https://www.hsfkramer.com/en_US/notes/data/2024-posts/EDPB-Opinion--How-far-down-the-supply-chain-do-controller-duties-extend--

24 European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://www.edpb.europa.eu/system/files_en?file=consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

25 European Union, General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

processing activity. A manufacturer that independently determines the purposes and essential means of collecting, retaining, disclosing, or otherwise using user data is likely to be a controller, or possibly a joint controller, for that activity. By contrast, a manufacturer may have a stronger claim to processor status where it processes data solely on behalf of an identified controller, within a defined scope, and only on that controller's documented instructions.

User-facing mechanisms that allow individuals to grant, scope, and revoke permissions can help satisfy consent requirements that apply to neural-data processing under emerging state laws. The strongest designs support clear, affirmative, informed, and purpose-specific consent; provide separate choices for materially different uses or third-party disclosures where required; and make withdrawal or revocation workable. [26] The exact requirements vary by jurisdiction, and consent controls must be paired with required notices, purpose limitations, data-protection assessments, deletion practices, and downstream-sharing controls. While user-facing mechanisms support privacy-by-design and satisfy consent requirements under emerging neurodata regulations, they do not assign the individual as the data controller or data processor.

Controllers still bear primary accountability, while processors retain independent GDPR duties and may face direct liability if they exceed lawful instructions or breach processor-specific obligations.[27]

> *The GDPR is designed to give data subjects meaningful control over personal data relating to them. It does so through enforceable rights to transparent information, access, rectification, erasure, restriction, objection, data portability, consent, and the ability to give, refuse, and withdraw consent. These rights can support a user-controlled permissions architecture, including the ability to scope or revoke access. They do not, however, by themselves give the data subject legal "custody" of the data or make the user the controller; the organization that determines the purposes and essential means of processing remains responsible as controller.*[28]

Insurance underwriting considerations are likely to evolve as liability risks associated with neural data collection, use, disclosure, and security become more pronounced. Cyber insurers increasingly seek evidence that security and privacy controls are implemented and effective. For manufacturers who handle sensitive personal data, demonstrable data-governance practices such as documented consent and permission controls, data-flow records, vendor oversight, access management, and independent audit or certification may strengthen an underwriting submission and may support more favorable terms, limits, and pricing.

---

26 KFF Health News, States Pass Privacy Laws To Protect Brain Data Collected by Devices, https://kffhealthnews.org/mental-health/colorado-california-montana-states-neural-data-privacy-laws-neurorights/

27 European Data Protection Board, Data Controller or Data Processor, https://www.edpb.europa.eu/sme/learn-the-basics/data-controller-or-data-processor_en

28 European Union, General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

8. 2026 Privacy and Data-Governance Checklist

- Identify every legal regime in the areas of privacy, health data, biometric, AI, and neural data that applies to your product today. Include state biometric laws, HIPAA where applicable, the GDPR and EU AI Act where applicable, and emerging neural data specific laws.
- Assess the current consent experience against a granular, purpose-specific, and readily revocable standard, not merely a one-time EULA or general terms acceptance.
- Inventory all current and planned OEM, licensing, platform, and data-sharing relationships. Confirm that consent, access-control, security, retention, and downstream-use obligations apply consistently throughout those relationships.
- Compare an in-house build with third-party infrastructure based on the full lifecycle cost, including compliance operations, audits, vendor management, security maintenance, and continuous monitoring of regulatory changes.
- Review the organization's legal role and risk allocation with counsel. In particular, determine whether the data architecture and operating model support a defensible controller, processor, or joint-controller position for each processing activity.
- Review this checklist at least annually to update the regulatory and data-flow assessment; and sooner following material changes to the product, marketing practices, partnerships, or applicable law. Privacy rules for biometric, health, AI, and neural data are developing rapidly; a point-in-time assessment will not remain sufficient indefinitely.

9. Closing

Neural data compliance in 2026 reflects the early stage of many emerging technology regulatory regimes consisting of overlapping laws, limited precedent, and meaningful consequences for missteps before the legal framework is fully settled. Manufacturers need not resolve every issue at launch, but they should treat compliance as a continuous governance function and not a one-time box to check.

FISE Technologies is developing identity, consent, and data-governance infrastructure tailored to neural data and other continuously generated sensitive data for manufacturers, their partners, and end users. If this guide raises questions about your product, data architecture, partnerships, or roadmap, we are available to help you navigate and implement a solution, whether building in-house or exploring shared, auditable infrastructure.

Contact: support@fise.tech