Written Testimony of IQVIA
Regarding Vermont House Bill 211
An Act Relating to Data Brokers and Personal Information

Submitted to: Senator Alison Clarkson
Chair, Vermont Senate Committee on Economic Development, Housing and General Affairs

Introduction and IQVIA's Role in Healthcare Data

On behalf of IQVIA, I appreciate the opportunity to submit written testimony on Vermont House Bill 211, *An act relating to data brokers and personal information*. IQVIA is a leading global provider of advanced analytics, technology, and research services for the healthcare and life sciences sectors. For decades, IQVIA has supported healthcare stakeholders through the responsible use of information, analytics, and technology to advance healthcare delivery, public health, and patient outcomes. Our work enables regulators, healthcare providers, researchers, and life sciences companies to better understand healthcare systems, improve the safety and effectiveness of treatments, and inform healthcare policy.

For clarity, this testimony focuses on IQVIA's U.S. syndicated information services ("Healthcare Data Services"), which are based on the use of de-identified data and are subject to applicable U.S. legal and regulatory requirements. IQVIA's Healthcare Data Services are supported by privacy-enhancing technologies, established governance frameworks, and operational safeguards designed to enable legitimate healthcare, research, regulatory, and public health uses of data while appropriately managing risk. De-identification occurs prior to IQVIA's receipt of the data, and IQVIA maintains controls designed to ensure that the data does not reasonably identify individual patients.

IQVIA[1] has been registered as a data broker in Vermont and other jurisdictions for many years and has decades of experience operating under a wide range of privacy, data broker, and related regulatory regimes. In the context of IQVIA's Healthcare Data Services, this registration reflects transparency regarding the handling of healthcare professional (HCP) professional data and should not be understood to imply the brokerage of identifiable patient information.

Overview of IQVIA's Position on House Bill 211

IQVIA supports the objectives of Vermont's data broker law and appreciates the legislature's focus on enhancing transparency and consumer privacy protections. At the same time, as currently drafted, House Bill 211 risks extending consumer-oriented data broker obligations to categories of data—particularly healthcare professional data—that play a critical role in healthcare delivery, patient safety, and regulatory compliance, and that have historically been treated differently under other privacy and consumer protection frameworks.

[1] Within the IQVIA family of companies, IQVIA Digital supports certain activities, including the management of healthcare professional (HCP) data in the context of IQVIA's Health Data Services. IQVIA Digital is the current registrant as a data broker in Vermont. In prior years, IQVIA itself served as the registered data broker in Vermont. Importantly, neither IQVIA nor IQVIA Digital acts as a data broker with respect to patient data. IQVIA's patient-level healthcare data assets are based on de-identified information, which does not constitute personal information of a consumer under Vermont's data broker framework. For convenience, we will simply refer to IQVIA and IQVIA Digital in this testimony as "IQVIA".

Accordingly, IQVIA respectfully seeks targeted clarifications to House Bill 211, summarized at a high level below and described in greater detail in the attached document titled "Proposed Changes Requested by IQVIA." These clarifications are intended to preserve the bill's consumer privacy goals while avoiding unintended consequences for healthcare systems.

High-Level Summary of Requested Clarification

IQVIA requests clarification that information about individuals acting in a professional or business capacity—particularly healthcare professionals—should not be treated as consumer personal data for purposes of deletion, opt-out, or related consumer-directed rights. Treating HCP professional data as consumer data would diverge from established legal distinctions and risk disrupting essential healthcare functions.

Why These Clarifications Matter

Patient Safety, Pharmacovigilance, and Risk Management

Healthcare regulators and life sciences companies rely on established pharmacovigilance and patient protection programs—such as the FDA's Adverse Event Reporting System (FAERS), required post-marketing adverse event follow-up under federal regulations, and Risk Evaluation and Mitigation Strategies (REMS)—to identify, assess, and respond to potential safety risks associated with approved medicines. Each of these programs depends, in practical terms, on the availability of accurate healthcare professional data, including provider identity, specialty, and practice contact information, to support follow-up, clarification of reported events, prescriber education, and targeted safety communications. Treating such professional information as consumer personal data subject to deletion or opt-out requirements risks impairing these safety-related functions, with potential downstream effects on patient protection efforts. For neutral service providers like IQVIA that support these activities, restrictions on access to professional provider data could have direct downstream impacts on patient safety, an outcome that is unlikely to reflect legislative intent.

Regulatory Compliance and Healthcare Transparency

Federal and state laws impose mandatory transparency and reporting obligations on healthcare manufacturers and other stakeholders, including requirements to track and disclose payments or value transfers to healthcare professionals. These obligations are designed to promote accountability and public trust. Treating HCP professional identifiers as consumer personal data subject to deletion could create conflicts between Vermont's data broker requirements and existing legal obligations, leading to incomplete reporting or inconsistent records. Such outcomes would weaken transparency frameworks rather than strengthen them. Clarifying that professional data remains distinct from consumer data would help avoid these conflicts.

Public Health Research and Real-World Evidence

Public health research and the development of real-world evidence (RWE) rely on healthcare professional (HCP)–linked professional data to understand how healthcare is delivered outside of controlled clinical trials. In this context, professional data is used to contextualize de-identified healthcare activity, identify system-level trends, and evaluate public health interventions—not to profile healthcare professionals in their consumer or personal capacity.

Examples of HCP-linked professional data commonly relied upon in public health and RWE analyses include:

- Professional identifiers and credentials. Such as National Provider Identifier (NPI), licensure status, and specialty or sub-specialty, which are used to ensure that healthcare activity is attributed to the appropriate type of provider (for example, distinguishing primary care from specialty care).
- Practice setting and facility affiliation. Including hospital affiliation, medical group membership, and care-setting indicators (such as inpatient, outpatient, or ambulatory care), which allow researchers to assess how care delivery varies across settings.

- Provider specialty and scope of practice. Specialty classifications are used to evaluate whether treatments are being prescribed or administered in a manner consistent with clinical guidelines, approved indications, or public health recommendations.

- Geographic and regional indicators. Aggregated location information (for example, state, region, or rural versus urban classification) supports analyses of geographic variation in access to care, disease burden, or treatment uptake, including during public health emergencies.

- Role within care pathways or treatment networks. Professional role indicators help researchers understand how patients move through healthcare systems — for example, from diagnosis to treatment and ongoing monitoring.

- Provider-level linkage to support aggregation and de-identification. HCP professional data is often used as an anchor to aggregate patient-level information at a practice, facility, or specialty level, enabling population-level analyses while maintaining patient de-identification.

While some elements of this information may be available from public sources, publicly available HCP data is frequently incomplete, outdated, fragmented, or internally inconsistent. Providers change practice locations, affiliations, specialties, and care settings with regularity, and public records often lag behind real-world conditions or contain duplicative or erroneous entries. Companies like IQVIA play an essential role in addressing these limitations by systematically validating, standardizing, reconciling, and updating professional healthcare data so that it can be reliably used for public health research and real-world evidence development. Absent these data stewardship efforts, HCP-linked data is often unsuitable for longitudinal analysis, trend identification, or regulatory-grade research.

These forms of HCP-linked professional data are therefore essential to monitoring real-world utilization and effectiveness of therapies, identifying unwarranted variation in care, supporting disease surveillance, and evaluating public health and regulatory interventions after approval—uses that are expressly contemplated in federal real-world evidence frameworks. Treating such professional information as consumer personal data subject to deletion or opt-out mechanisms risks fragmenting datasets and undermining analytic validity, while providing little additional privacy protection—particularly where patient information is already de-identified.

Unnecessary Compliance Burdens with Limited Privacy Benefit

Much HCP professional information—such as licensure status, practice address, or professional affiliation—is already publicly available or integral to healthcare operations. Subjecting this

information to consumer-oriented deletion and consent mechanisms would impose substantial operational burdens on healthcare data users with minimal incremental privacy benefit.

Resources devoted to processing deletion requests for professional data would be better directed toward safeguarding genuinely sensitive personal information. Targeted clarification in H.211 would enable a more proportionate and risk-based regulatory approach.

Consistency with Established Legal and Policy Norms

Long-standing legal frameworks in the United States consistently distinguish between information associated with individuals acting in a personal or household capacity and information associated with individuals acting in a professional or business capacity. This distinction appears across a wide range of statutes, including consumer protection, financial services, employment, and privacy laws, and reflects a policy judgment that professional context data generally presents different—and lower—privacy risks than personal consumer data.

For example, federal statutes such as the Gramm-Leach-Bliley Act[2], the Truth in Lending Act[3], and the Fair Debt Collection Practices Act[4], refer to "consumer" by reference to personal, family, or household purposes, expressly excluding business or professional activities. State medical confidentiality laws and their enforcement have a long history of prioritizing patient confidentiality and not recognizing a privacy right for healthcare professionals. More recent comprehensive state privacy laws similarly reflect this distinction, often through exclusions or limitations for employee data, business-to-business contact information, or information processed in a professional context. These laws reflect a more risk-based and contextual approach to privacy regulation, recognizing that not all data about individuals warrants the same regulatory treatment.

By contrast, state data broker registration laws—particularly those modeled closely on California's framework—more frequently blur or collapse this distinction, resulting in professional contact and work-related information being swept into consumer-oriented regulatory regimes. This approach appears to be less the product of a deliberate, risk-based policy choice and more a consequence of how California's data broker law emerged. California's framework was developed in the shadow of a threatened ballot initiative, which compressed legislative timelines and constrained opportunities for more tailored drafting. That process produced a statute that prioritizes broad coverage and administrative visibility, but does so without fully differentiating among data types or contexts. Many subsequent state data broker laws have relied on California's structure as a template, and in doing so have replicated this lack of nuance, even as other areas of privacy law in the U.S. have evolved toward more differentiated and balanced approaches. Vermont's consideration of House Bill 211 presents an opportunity to avoid carrying forward that structural limitation, particularly where healthcare professional data is concerned.

---

[2] "Consumer means an individual who obtains or has obtained a financial product or service from [a financial institution] that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. 16 CFR §134.2(b)(1)

[3] "Concept of 'consumer' is "primarily for personal, family, or household purposes." 15 U.S.C. §1602(i).

[4] The term 'consumer' means any natural person obligated or allegedly obligated to pay any debt." and "Debt" is defined as an obligation of a consumer "to pay money arising out of a transaction…primarily for personal, family, or household purposes." 15 U.S.C. 1692a(3) and (5).

Failing to maintain a clear distinction between consumer personal data and professional healthcare data risks placing Vermont's data broker regime at odds with broader privacy and consumer protection norms. More importantly, it risks regulating low-risk professional information in ways that complicate healthcare operations, patient safety activities, and regulatory compliance—without meaningfully advancing consumer privacy protection.

Clarifying House Bill 211 to preserve the established separation between consumer data and healthcare professional data would better align Vermont's law with the risk-based principles reflected across the wider privacy landscape in the U.S., while still supporting transparency and accountability in the data broker ecosystem.

Conclusion

IQVIA appreciates the legislature's efforts to strengthen consumer privacy protections through House Bill 211. We respectfully submit that targeted clarifications regarding healthcare professional information are necessary to ensure the bill achieves its intended goals without unintended harm to patient safety, public health, and healthcare transparency.

The proposed changes summarized above—and detailed in the attached document—would preserve consumer protections while recognizing the distinct role that professional healthcare data plays in supporting healthcare delivery and oversight. IQVIA stands ready to continue working constructively with the Committee and other stakeholders as this legislation moves forward. Thank you for the opportunity to share our perspective.

Respectfully submitted,

Harvey Ashman
Senior Vice President & Deputy General Counsel
IQVIA

Attachment: *Proposed Changes Requested by IQVIA*

IQVIA proposed changes to HB 211 (additions underlined):

- §2430(3)(B). "Brokered personal information" does not include (i) publicly available information, (ii) information about an individual acting in a professional, occupational, or business role, (iii) information about organizations and individuals as business representatives, and (iv) information about service providers in third-party reviews.

- §2430(5). "Consumer" means an a natural person residing in this State and acting in a personal, family or household capacity and does not include: (A) individuals acting in a business or professional capacity; (B) employees, contractors, or agents acting within the scope of their role; (C) representatives of a business or organization; or (D) information derived from or used primarily in commercial, professional, or employment contexts.

//////////////////////////