Date: **May 1, 2026**
To: **Chair Marcotte and Members of the House Committee on Commerce and Economic Development**
From: **Coalition of Vermont Health Care Organizations (signatories below)**
Re: **S. 71 - An act relating to consumer data privacy and online surveillance**

Our organizations are made up of and represent health care providers who use health care data on a daily basis to improve patient care and health outcomes in our state -and all are already subject to a number of federal and state data privacy laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA).

We are writing to submit our opposition to Draft 2.3 of S. 71, An act relating to consumer data privacy and online surveillance, and in support of S. 71 as passed the Senate in 2025.

Our organizations consider the privacy and security of an individual's health data to be critical to the work we do and support the goals providing consumers rights and protections over their personal information, just as HIPAA-covered entities are already held at a high standard for the privacy and security of protected health information.

We know you are likely familiar with the HIPAA standards related to protecting health information. For a helpful overview, see the Health and Human Services (HHS) Overview of the HIPAA Privacy Rule,[1] outlining the requirements that apply to HIPAA-covered entities, including:

- issuing a notice of privacy practices to all patients regarding how data is protected;
- obtaining patient authorization for many uses of data;
- limiting use of data to the "minimum necessary;"
- employee training regarding HIPAA privacy requirements;
- applying HIPAA requirements to "business associates" of HIPAA-covered entities – this includes all business partners that receive protected health information, such as entities that store patient records, create patient websites or portals, process payments and more;
- providing guidance related to how HIPAA applies to website and tracking technologies;[2]
- enforcement for noncompliance for HIPAA-covered entities and business associates[3] including significant penalties for violations – to date, HHS' Office of Civil Rights has imposed civil money penalties of $144,878,972 for HIPAA violations;[4]
- breach notification requirements.

Separate comprehensive rules under HIPAA require that health care entities protect the data security of electronic information and address cybersecurity (the "Security Rule")[5] and require notification of breaches (the "Breach Notification Rule").[6]

Vermont in state law has adopted HIPAA as the standard for covered entities – see 18 V.S.A. § 1881. As health care services in Vermont become more integrated, many covered entities in Vermont are also subject to federal regulation 42 CFR Part 2, which outlines further standards for managing and sharing substance use disorder treatment records.[7]

---

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#
[2] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
[3] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html
[4] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
[5] https://www.hhs.gov/hipaa/for-professionals/security/index.html
[6] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[7] https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-part-2/index.html

Our organizations have asked and have yet to be presented with concrete, non-hypothetical examples of how HIPAA is insufficient to protect Vermonters' health care data and why additional regulation is necessary for health care entities in Vermont.

Our organizations support the approach taken in S. 71, exempting HIPAA-covered entities from additional regulatory burden. As drafted, the exemptions in S. 71 Draft 2.3 section 2415c fall short of meeting the needs of Vermont's health care organizations and will lead to both high consumer confusion and high compliance costs.

Consumer confusion

By only exempting certain types of data, and applying the bill's requirements to all controllers that possess even one consumer's sensitive data, S. 71 Draft 2.3 will require health care providers to comply with both HIPAA and the new consumer privacy requirements. Health care providers have already seen firsthand the consumer confusion created by applying two similar but different sets of privacy requirements to patient data. Currently, providers must comply with both HIPAA for "protected health information" and federal regulations found at 42 CFR Part 2 for substance use disorder treatment records. Historically, this has led not only to barriers to care but confusion for patients such as with whom their records can be shared, in which circumstances data can be shared, and when an authorization is required. The federal government now realizes the shortcomings of two similar but not aligned standards and in 2024 released updated 42 CFR Part 2 regulations to try to align the sharing of and access to 42 CFR part 2 data more closely to HIPAA.[8]

Compliance costs

Small health care entities will need to complete a comprehensive legal and operational analysis of what data they hold that is exempt under the statute as part of a "health care record" or what data is covered. This takes time and resources away from the mission work of organizations with tight budgets and already tapped capacity. The required investments will disproportionally impact small Vermont-based health care organizations compared to a large corporation. Compliance is particularly complicated by many Vermont health care practices serving patients from multiple states, making consistency with other state data privacy laws, which *do* include HIPAA-covered entity exemptions, important.[9]

Health care providers already invest in data security and privacy. This bill would impose new costs without clear benefit beyond what already exists. Recent educational sessions for small businesses in Vermont cite compliance costs of $20-40,000 with estimates from the Vermont Legislative Research Service for complying with California's privacy law ranging from $50,000 for a business of 20 employees to $100,000 for a medium businesses of 20-100 employees.[10] This does not factor in the unique needs of analyzing how to reconcile HIPAA compliance with consumer data privacy compliance. Many health care entities in Vermont – including health centers, designated agencies, and home health organizations – are already running at an operating loss. You have no doubt read the reports of primary care offices closing in Rockingham,[11] Waitsfield,[12] and Stowe[13] due to budget pressures. Depending on the payment structure for each organization, additional compliance costs either get passed along to consumers in the form of health care premiums, the state if Medicaid reimbursement adjusts, or ultimately, a reduction in health care services to Vermonters or the closure of organizations.

---

[8] https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/fact-sheet-42-cfr-part-2-final-rule/index.html

[9] Pending Mass Bill S. 2608 includes both a smaller entity and data type exemption for HIPAA-covered entities; New Hampshire exempts HIPAA covered entities; CT adopted amendments exempt HIPAA-covered entities.

[10] https://www.uvm.edu/d10-files/documents/2025-12/Data-Privacy-Regulation.pdf

[11] https://vtdigger.org/2025/02/28/very-very-financially-fragile-vermonts-federally-qualified-health-centers-are-struggling/

[12] https://mrvhealthcenter.org/clinic-closing/

[13] https://vtdigger.org/2025/02/07/lamoille-health-partners-to-close-stowe-practice/

To take effective action to ensure consumer data is protected, to address the needs of HIPAA-covered entities to engage in appropriate uses of data, as well as to sustainably operate to meet the health care needs of Vermonters, we respectfully request the committee support S. 71 as passed the Senate in 2025.

Sincerely,

Jessa Barnard
Executive Director, Vermont Medical Society
jbarnard@vtmd.org

Jessica Barquist
Vice President of Public Affairs, VT, Planned Parenthood of Northern New England
Jessica.Barquist@ppnne.org

Eric Covey
Interim Executive Director, VNAs of Vermont
eric@vnavt.org

Randy Farmer
President & CEO, VITL
RFarmer@vitl.net

Devon Green
VP of Government Relations, Vermont Association of Hospitals and Health Systems
devon@vahhs.org

Amy Johnson
Director of Government Affairs and Communications, Vermont Care Partners
amy@vermontcarepartners.org

Helen Labun
Executive Director, Vermont Health Care Association
laura@mmrvt.com

Mary Kate Mohlman
Director of Vermont Public Policy, Bi-State Primary Care Association
mmohlman@bistatepca.org

Susan Ridzon
Executive Director, HealthFirst Independent Practice Association
sr@vermonthealthfirst.org

Michelle Wade
President, Vermont Nurse Practitioners Association
mwadenp@gmail.com

Stephanie Winters
Executive Director, Vermont Academy of Family Physicians; American Academy of Pediatrics- VT Chapter; VT Psychiatric Association
swinters@vtmd.org