Date: April 19, 2024

To: Chair Lyons and Members of the Senate Health & Welfare Committee

From: Coalition of Vermont Health Care Organizations (signatories below)

Re: H. 121- Request for Exempting HIPAA-Covered Entities

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 understand that your committee has been asked to weigh in regarding H. 121's impacts on health care entities.

Our organizations request: The exemption for protected health information be rewritten to exempt HIPAA-covered entities and business associates – in line with the majority of states with data privacy laws,[1] as follows:

> *§ 2417. EXEMPTONS*
> *(a) This chapter does not apply to:*
> *(2) a covered entity or business associate, as defined in 45 CFR 160.10.*

The current draft of H. 121 exempts a number of entities because they are subject to other federal or state privacy laws.[2] The Senate Economic Development Committee deferred the decision about HIPAA-covered entities to your committee. **HIPAA-covered entities are already subject to comprehensive federal law and regulations related to data privacy and security and must be exempt to minimize consumer confusion and compliance costs, as elaborated below.**

Our organizations support the goals of H.121 and consider the privacy and security of an individual's health data to be critical to the work we do. We support the design of H. 121 to hold consumer health data to a higher standard than other data (Section 2428), just as HIPAA-covered entities are held at a high standard for the privacy and security of protected health information.

We know you are 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[3], outlining 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;"

---

[1] Virginia, Connecticut, Utah, Tennessee, Montana, Florida, Texas, Iowa, and Indiana, contain an entity-level exemption for HIPAA covered entities. Further, if a healthcare provider is a nonprofit, then they will be completely exempt in every state except for Colorado, Delaware, Oregon and New Jersey. See for example, CT Data Privacy Act Section 3 (https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF) and https://www.dwt.com/blogs/privacy--security-law-blog/2023/10/consumer-data-privacy-laws-healthcare-phi

[2] Entities exempt in H. 121 now include financial institutions and credit unions § 2417 (a)(14); insurance companies (a)(15); third party administrators (a)(16); public service companies (a)(18) and institutions of higher education (a)(19).

[3] https://www the.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#

- employee training regarding HIPAA privacy requirements;
- application of HIPAA requirements to "business associates" of HIPAA-covered entities;
- application of HIPAA requirements (e.g. limits on disclosures) to online tracking technologies on websites and mobile apps;[4]
- enforcement for noncompliance;
- breach notification requirements.

There is a second federal rule under HIPAA dealing entirely with health care data security,[5] which requires safeguards to be in place to ensure appropriate protection of electronic protected health information. 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.[6]

The House recognized the strength and sufficiency of HIPAA law and regulation and did exempt data processed in compliance with HIPAA (see § 2417 (a)(2) and (8)). However, as drafted, this exemption still falls short of meeting the needs of Vermont's health care organizations and will lead to both high consumer confusion and high compliance costs. Data arguably not squarely covered by this exemption – though a full legal analysis would be required by each organization - includes volunteer records, community and patient surveys, community newsletter lists, certain website data and vendor contracts. These are all records necessary for the basic functioning and fiscal solvency of Vermont's health care entities – from home health and long-term care facilities to adult days, health centers, small independent medical and mental health practitioners to Vermont's nonprofit hospitals. Entities protect these records through best practices, including depending on third-party services that are PCI compliant (that meet Payment Card Industry Data Security Standards) to accept donations and payments and Customer Relationship Management (CRM) software, databases, or third-party services to securely store and manage personal data.

Consumer confusion

Other organizations have posited that two different data privacy requirements could lead to confusion, but health care providers have already seen firsthand that applying two similar but different sets of privacy requirements to patient data obstructs confuses patients when required to comply with both HIPAA and 42 CFR Part 2. 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 just last month 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.[7]

Under H. 121, as just one example of the conflict, a HIPAA covered entity would need to provide differently worded notices to individuals where one notice would tell them that they have a right to delete data (H. 121), and the other notice would not include a right to delete data while explaining how their data is protected (HIPAA). It is not even clear how health care entities would provide a notice in situations such as a general community survey regarding quality of services or health care services

---

[4] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
[5] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[6] https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-part-2/index.html
[7] https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/fact-sheet-42-cfr-part-2-final-rule/index.html

desired – as required of hospitals in their community needs assessments – when handing out surveys in situations such as farmer's markets and community health fairs.

Compliance costs

Small health care entities will first need to complete a comprehensive legal and operational analysis of what data they hold that is exempt under the statute and what data is covered. The organization will then have to complete an analysis of how and whether they can protect this data under HIPAA. It is unclear exactly how HIPAA standards would be used to cover donor data, for example. Would a HIPAA notice of privacy practices be given to each donor? Would an authorization need to be signed to publicly share donor data on a donor recognition list? If data does have to be protected under H. 121, organizations will then need to make significant updates to their existing data policies, data management practices, and even technology.

This takes time and resources away from the mission work of organizations with tight budgets and already tapped capacity. Further, any general implementation guidance created for small businesses or Vermont organizations as a whole regarding compliance with H. 121 will likely not be specific enough to assist health care organization in this analysis. The required investments will disproportionally impact small Vermont-based health care organizations compared to a large corporation. According to Common Good Vermont, in Colorado, there have been organizations that have had to spend up to $40,000 on consultants to help them comply with new regulations. Many health care entities in Vermont – including health centers, designated agencies, long-term care facilities and home health organizations – are already running at an operating loss. 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.

Thank you for considering the requested modifications to H.121. Please do not hesitate to contact any of us if you have any questions or would like additional information.

Sincerely,

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

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

Beth Anderson
President & CEO, VITL
banderson@vitl.net

Jill Mazza Olson
Executive Director, VNAs of Vermont
Jill@vnavt.org

Stephanie Winters

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

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

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

Susan Ridzon
Executive Director, Health First
sr@vermonthealthfirst.org

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

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