Date: Updated March 11, 2024 to reflect draft 7.1

To: Rep. Michael Marcotte, Chair, House Committee on Commerce & Economic Development
Rep. Monique Priestley, Clerk, House Committee on commerce & Economic Development
Members of the Vermont House Committee on Commerce & Economic Development

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

Re: H. 121- Comments and Proposed Modifications Updated to Reflect Draft 7.1

Our organizations are made up of and represent health care providers and the state health information exchange – all of whom use health care data on a daily basis to improve patient care and health outcomes in our state -and all are 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 in relation to H.121, an act relating to enhancing consumer privacy. Specifically, we are submitting an update to our initial comments, which we provided on February 18th. This new letter reflects changes that have been made in draft 7.1, which was distributed after our initial letter. In addition, we've included a list of examples of how this bill creates different requirements for managing patient data for health care organizations. Updates in this version are indicated with red font.

We appreciate the committee's willingness to consider comments about the proposed bill. Our comments below are modified to reflect where changes have been made. However, our primary concern regarding the need to expand the exemptions to include HIPAA covered entities and their business associates remains.

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 2425), just as HIPAA-covered entities are held at a high standard for the privacy and security of protected health information.

We know you are well aware of 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, outlining the requirements that apply to HIPAA-covered entities, including: a notice of privacy practices; when patient authorization is required for the use of data; limiting use of data to the "minimum necessary;" how all of these restrictions also apply to "business associates" of HIPAA-covered entities; enforcement for noncompliance; and breach notification requirements: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#. 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 42 CFR Part 2, which outlines further standards for managing and sharing substance use disorder treatment records.

To address both (1) the needs of HIPAA-covered entities to engage in appropriate uses of data and (2) to ensure that health data is adequately protected, we respectfully request the following changes in the bill:

Definition Alignment and Clarification

- § 2415 (1): Align the definition of "Abortion" with the existing statutory definition at 9 VSA § 2492 (in agreement with Planned Parenthood of Northern New England). –
    - Update: this is addressed in draft 7.1

- § 2415 (9): Align the definition of "consumer health data" to HIPAA. The proposed definition directs the protections that controllers must apply to this data. Currently the definition only includes "personal data that a controller uses to *identify* a consumer's physical or mental health condition or diagnosis…." However, a controller can misuse consumer health information even if it is not being used to *identify* a consumer's health condition – for example the fact that an individual has taken a specific prescription drug or visited a health care provider -- even if this fact is not linked to a diagnosis. We recommend aligning more closely to the HIPAA definition of "individually identifiable health information" (45 C.F.R. § 160.103), which includes:

  > *Information that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual.*

  - Update: This has not been addressed in draft7.1 – although under "sensitive data" at (44)(F), consumer health now specifies it includes data related to past, present or future mental or physical health condition or treatment

- § 2415 (12): Clarify, perhaps in the definition of "controller" - or in definition (29), "process" - whether the applicability of the bill is only to *electronic* data or also applies to *paper* records. Nowhere is this specified and could have very different impacts on entities in Vermont depending on this scope.
  - Update: this was not addressed in draft 7.1 and remains a concern.

- § 2415 (36) Align definition of reproductive health care with 1 V.S.A. § 150(c)(1) (in agreement with Planned Parenthood of Northern New England).
  - Update: this has been reflected in draft 7.1.

Equitable Application of Exemption for Number of Consumers

- § 2416 – Applicability – clarify that the application only to persons who control or process the data of not fewer than 6,500 consumers (or 3,250 consumers if 20% of gross revenue is derived from sale) does not count the number of consumers/consumer records that are exempt under § 2417. Without such clarification, the impacts of the bill would be disproportionately felt by small organizations who largely control exempt records. For example, a small nonprofit that does not work in the health field can control the records of 6,500 potential donors and reach out to those donors for donations. Other examples of records held could include consumer and community surveys, website data and vendor agreements with third parties. However, if a health care entity holds 6,500 health care records, they could be pulled into the full applicability of the bill for any 1 additional record of this type held.
  - Update:this was not addressed in draft 7.1 and remains a concern.

Limit Confusion About Privacy Laws, Which Acts as a Barrier to Integrated and Coordinated Care

- Update: this was not addressed in draft 7.1 and remains a significant concern.

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 necessary care. As mentioned above, in addition to HIPAA, there are different privacy requirements applied to patient records

related to substance use treatment outlined in 42 CFR Part 2. It has proven[1] a barrier to offering coordinated and integrated care when practices do not have full data regarding medications and care a patient may be receiving elsewhere. The federal government is now walking back this position and has just this 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.[2]

Vermont is different than other states in that it is moving towards paying health care providers based on how well they coordinate care and address needs such as housing, transportation and food insecurity. In doing this work, health care providers mix medical and non-medical records. The additional exemption in § 2417 (a)(7) is not sufficient to cover these types of data received by HIPAA-covered entities as it may not be "so intermingled as to be indistinguishable from" protected health information. Under the proposed version of H.121, Vermont's health care organizations (covered entities and business associates) could be forced to manage data about individuals that is received from sources other than health care providers in a manner that impedes the coordination of care.

Following are examples of how the bill as currently drafted could impact health care entities:

1. Care coordinators often assist individuals in applying for food, housing, or other assistance programs. Collecting and transmitting this data is not considered PHI.
2. Data obtained regarding community resource capacity for housing, food, and other social needs not directly linked to a patient.
3. Information used to understand a service area's interests, concerns, health needs as part of the IRS required Community Health Needs Assessment, population health activities, and health care service planning.
4. Information used to enhance patient experience, payment, financial assistance, and prevent identify theft and fraud prevention.
5. Patient-generated health data submitted by a patient directly to a business associate (e.g. VITL), such as data from a remote heart monitoring device or a reading from a home blood pressure cuff is not PHI.
6. Social Determinants of Health data submitted by a community organization directly to a business associate (e.g. VITL), for example food insecurity or housing status, is not PHI.
7. Social determinants of health data (housing, food, transportation) gathered by a covered entity but not directly linked to patient care decisions (lack of clear regulatory guidance regarding whether this is PHI and also how "intermingled" it would have to be under H. 121).

§ 2417 (a)(1): The exemption for protected health information should be rewritten to exempt HIPAA-covered entities and business associates, as follows:

§ 2417. EXEMPTONS
(a) This chapter does not apply to:

---

[1] The Perceived Impact of 42 CFR Part 2 on Coordination and Integration of Care: A Qualitative Analysis Dennis McCarty, Ph.D., Traci Rieckmann, Ph.D., Robin L. Baker, M.P.H., K. John McConnell, Ph.D. Published Online:1 Nov 2016https://doi.org/10.1176/appi.ps.201600138

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

(1) a covered entity or business associate, as defined in 45 CFR 160.10 as long as the entity's primary function involves operating as a covered entity or business associate, and its operations that are unrelated to its functions as a covered entity or business do not represent a material part of its operations.[3]

...

(7) information that originates from and that is intermingled so as to be indistinguishable with, or information treated in the same manner as, information that is exempt under subdivisions (1) through (6) of this subsection (a) that is maintained by a covered entity, business associate, or a qualified service organization.[4]

Alternative: Including an exemption for entity-type will eliminate confusion for the entities as we perform our work, and for the patients whose health data we steward. However, we understand there may be discussion among the committee related to eliminating all entity-level exemptions already included in the proposed bill. If the committee moves forward with removing all entity-level exemptions, we request that the exemption be rewritten as follows:

§ 2417. EXEMPTONS

(a) This chapter does not apply to:

(1) all data related to a patient that is collected or maintained by a covered entity or business associate, as defined in 45 CFR 160.10 as long as the entity's primary function involves operating as a covered entity or business associate, and its operations that are unrelated to its functions as a covered entity or business do not represent a material part of its operations.[3]

...

(7) information that originates from and that is intermingled so as to be indistinguishable with, or information treated in the same manner as, information that is exempt under subdivisions (1) through (6) of this subsection (a) that is maintained by a covered entity, business associate, or a qualified service organization.[4]

Requiring HIPAA covered entities to operationalize compliance with a new state law that applies to different types of data would create a barrier to coordinated, integrated health care. We believe this would also create confusing expectations for individuals about how the data related to their health is managed and shared. A HIPAA covered entity would need to provide separate notices to patients where one notice would tell them that they have a right to delete health data, and the other notice would not include a right to delete health data while explaining that their health data can be accessed, used, and disclosed without authorization. The State's Health Information Exchange (VHIE) would need to deliver

[3] This language seeks to narrow the scope of an entity level exemption so that it only applies to entities that operate primarily as health care providers, payors, and organizations that support them such as VITL. This language seeks to exclude from the entity level exemption large information technology companies that serve as business associates for basic IT services such as cloud storage, but who have substantial operations that are unrelated to serving as a business associate.

[4] The language for this exemption is used by several states to avoid imposing overlapping compliance obligations by recognizing that HIPAA covered entities and business associates protect similar data in the same way even where a data element(s) may not fall within the HIPAA definition of protected health information. Such non-PHI data could include population health related data, or regional social determinates of health data, which may not be PHI if the data does not relate to an individual's treatment relationship with a covered entity. The language for this data exception appears in legislation in Connecticut, 42 C.G.S.A § 42-517(b)(9); Florida, XXXIII F.S.A. § 501.704; Iowa, XVI I.C.A § 715D.2; Montana, 30 M.C.A. 30-14-2804 §(2)(i); New Hampshire, SB 255-FN, 507-H-3, II. (i); Tennessee, 47 T.C.A. § 47-18-3311(a)(14); and Virginia, 59.1 § 59.1- 576(C)(8)

two different types of education to all Vermonters about how their data maintained in the VHIE is collected and shared, and would need to maintain multiple consent models to allow patients to opt out of how their different types of health data can be shared. Patients should have clarity about how their information will be protected, accessed, and used as they make informed decisions about contributing to their longitudinal health record as part of actively participating in their health care.

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

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

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

Mike Fisher
Chief Health Care Advocate, Office of the Health Care Advocate
mfisher@vtlegalaid.org

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

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