

# HEALTHCARE TRUST INSTITUTE

Submitted via email to [mstowellaleman@leg.state.vt.us](mailto:mstowellaleman@leg.state.vt.us)

April 2, 2024

Sen. Kesha Ram Hinsdale, Chair  
Senate Committee on Economic Development, Housing and General Affairs  
Vermont State House  
115 State Street  
Montpelier, VT 05633-5301

## **RE: H.121, An Act Relating to Consumer Privacy**

Dear Senator Hinsdale:

The Healthcare Trust Institute respectfully submits the below comments on H.121, An Act Relating to Consumer Privacy (H.121), to the Senate Committee on Economic Development, Housing and General Affairs (the Committee).

The Healthcare Trust Institute (HCTI) is an alliance of healthcare organizations committed to promoting and implementing effective privacy and security protections for health information that engender trust in the healthcare system and allow for the advancement of treatments, cures and improved healthcare quality for individuals and populations. HCTI members, which include companies and organizations from across the U.S. healthcare economy, agree that a strong national privacy standard for health information is needed to protect sensitive data and spur medical innovation.

HCTI strongly supports legislation to protect personal health data and provide consumers with basic rights with respect to their health data, including the right to know what personal health information about them is collected, the purposes for which it is collected, and the right to access and correct such information, among other things. HCTI members have supported, and continue to call for, federal legislation to provide these protections and rights for personal health data held by entities not subject to the Health Insurance Portability and Accountability Act (HIPAA).

We recognize and support the efforts to provide these rights and protections to Vermont consumers as reflected in H.121. We also support and appreciate that H.121 includes exemptions for certain types of entities and data, including protected health information (PHI) under HIPAA on the basis that these are already subject to other comparable privacy and security protections. This is necessary and appropriate to avoid imposing duplicative and potentially inconsistent requirements, which would not only make compliance more difficult, but could undermine data sharing needed for patient care.

We are concerned, however, that the HIPAA exemption in H.121 does not provide a clear and broad enough exemption, which will result in uncertainty and confusion, and expose HIPAA covered entities and their business associates (collectively, HIPAA entities) to potential liability under the bill. The reasons for this are twofold. First, the exemption is conditional on PHI being

processed in accordance with HIPAA or HIPAA documents, and second, the exemption applies only to PHI, and not to HIPAA entities. The conditional exemption means that, as a practical matter, HIPAA entities will fall under the jurisdiction of the agency (or court of law) enforcing H.121 to determine whether they are processing PHI in accordance with HIPAA, and then, if it is determined that a piece of PHI has not been handled in accordance with HIPAA, the extent to which the exemption is lost and for what time period. No HIPAA entity could operate effectively under such legal uncertainty, and the responsibility for determining and enforcing HIPAA compliance, including determining the consequences for non-compliance, should fall squarely and exclusively under the jurisdiction of the U.S. Department of Health and Human Services (HHS). Therefore, at a minimum, we urge the Committee to provide a clear and unconditional exemption for PHI. In addition, since “consumer health data” (as defined under H.121) held by a HIPAA entity is PHI and subject to HIPAA, HIPAA entities should be exempt from H.121, in the same way as the bill exempts financial institutions. Failure to do so creates confusion and uncertainty without adding any consumer protections. It is for this reason that most other states<sup>1</sup> enacting comprehensive data privacy laws provide exemptions for HIPAA entities. We recommend that Vermont to do the same in H.121.

We also ask that the Committee reconsider the provision that would allow enforcement of H.121 through a private right of action. While we fully support a robust enforcement mechanism to punish wrongdoers and deter violations, there are many effective mechanisms for doing so that will not have the significant unintended negative consequences that have historically accompanied a private right of action. For example, federal agencies such as HHS and the Federal Trade Commission (FTC) have proven to be very effective in enforcing data protections through resolution agreements that involve significant monetary payments and/or compliance plans and ongoing monitoring. This could be accomplished at the state level, including through the engagement of independent third parties to monitor ongoing compliance at the cost of the violating entity. These enforcement mechanisms ensure that regulatory agencies have control over the targeting and type of penalties imposed to achieve the policy goals of the legislation.

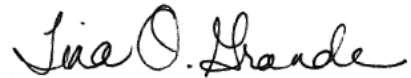
By contrast, a private right of action is a blunt enforcement instrument that has been seen to spawn indiscriminate, often frivolous, lawsuits calculated to extort payments in return for an end to time-consuming and costly litigation. Entities are not targeted with a goal of inducing compliance, but rather, based on deep pockets or other criteria germane to enriching the plaintiff's bar rather than enforcing the law or even compensating the consumers alleged to have been harmed. Not only have laws with a private right of action frequently failed to achieve the desired policy goals, but they have done the opposite by drawing resources and focus away from compliance to defending against lawsuits. They also have the effect of discouraging businesses from operating in the state as they factor in the increased costs, both financial and otherwise, of doing so in a litigious environment. We strongly urge the Committee to replace the private right of action with another more effective enforcement mechanism, such as those employed by HHS and the FTC.

---

<sup>1</sup> See, for example, the data privacy laws of Connecticut, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia.

Thank you for your consideration of our comments. Please do not hesitate to contact me at [tina@hctrustinst.org](mailto:tina@hctrustinst.org) or 202-750-1989 if you have any questions.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, looped "T" and "G".

Tina O. Grande  
President, Healthcare Trust Institute

Cc: Sen. Alison Clarkson, Vice Chair  
Sen. Randy Brock  
Sen. Ann Cummings  
Sen. Wendy Harrison, Clerk