To: The Senate Government Operations Committee

From: The Vermont Association of Hospitals and Health Systems, Vermont Health Care Association, Vermont Medical Society, VNAs of Vermont, Vermont HealthFirst, Bi-State Primary Care Association, American Academy of Pediatrics Vermont Chapter, Vermont Academy of Family Physicians, Vermont Psychiatric Association

Date: April 10, 2023

Re: Joint Comments Regarding H. 291

Thank you for considering these joint comments of the health care provider associations listed above.

The bill as passed by the House includes a provision that would require the Green Mountain Care Board to develop cybersecurity standards relating to health care. We did not have an opportunity to testify in the House and appreciate this opportunity to provide input.

We propose replacing the health care provision with language clarifying that the health care industry shall be subject to the extensive security standards already required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Health care organizations are already obligated under federal law to implement cybersecurity measures and have been since the first security rule was adopted in 2003. The federal government updates its strategy on security for health care entities' data and increases compliance through actions such as the HITECH Act and ongoing implementation guidance. The US Department of Commerce National Institute of Standards and Technology publishes extensive guidance and is currently promulgating new guidance. Health care organizations also carry cybersecurity insurance. Insurers make extensive and detailed demands on insured entities based on the most current information on mitigating cybersecurity risk.

In our view, the Green Mountain Care Board is not the appropriate body to develop or consider cybersecurity standards for HIPAA covered entities. The Board would need to build or purchase cybersecurity expertise, and their scope is limited to hospitals, ACO, and insurance companies. Home and community-based providers are outside their purview and expertise. Given the extensive federal law, regulation and guidance already available, this seems like an inefficient use of state resources.

Federal Security Standards

An overview of the HIPAA Security Rule and links to the rule and resources is available HERE. "The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

A summary of the original rule is HERE.

The cybersecurity guidance page for professionals HERE shows examples of ongoing updates.

NIST Special Publication 800-66, Revision 2: The most recent NIST standards (still in draft form), formally titled *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide*

Proposed Language

(b) Standards for other regulatory bodies. The cybersecurity standards approved by the Council pursuant to subsection (a) of this section shall include:
(1) cybersecurity standards developed by the Public Utility Commission to protect the State's critical infrastructures relating to electric, water, telecommunications, and any other essential sectors as determined by the Commission.
~~(2) cybersecurity standards developed by the Green Mountain Care Board to protect the State's critical infrastructures relating to health care, including hospitals, health care systems, accountable care organizations, and other essential health systems as determined by the Board~~
(2) Cybersecurity standards for covered entities required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).