VERMONT MEDICAL SOCIETY

To: **Members of the House Judiciary Committee**

From: **Paul Harrington, Executive Vice President**
Jessa Barnard, Vice President for Policy

Date: **April 21, 2016**

Re: **Vermont Medical Society Position on S. 155, Section 1, adding breach publication to website**

On behalf of Vermont's physicians, the Vermont Medical Society opposes any addition to S. 155 that would require medical practices to publish information regarding breaches on their individual practice websites. Our opposition in based on the following reasons:

1. **The requirement is unnecessary.** Under Vermont's Security Breach Notice Act, 9 V.S.A. § 2430 and 2435 and the federal HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, physician practices are already required to notify all affected individuals, and, as applicable, the Attorney General's office and the Office of Health and Human Services in the event of a data breach. See below for further details.
2. **The requirement adds administrative burdens to physician practices.** Physician practices are already required to interpret two separate breach notification schemes, with different definitions of breach, data covered and notification requirements. This would add a third requirement to already overwhelmed medical offices.
3. **The requirement would unnecessarily single out health care entities.** The proposed addition would require only health care entities to publish information about breaches to their websites – not financial institutions or others who may hold equally or more sensitive personal and financial data and are covered by Vermont's Security Breach Notice Act. Affected individuals are already notified and breaches are already published to the Attorney General or HHS website, as applicable. This additional requirement appears to simply be punitive in nature.
4. **The requirement is lacking clarity.** Existing breach notification laws have detailed definitions of a breach, the data covered, the effect of encrypting the data, timelines for notifying the affected individuals and regulatory entities, required content for the notice and more. The proposed amendment lacks necessary clarity and practices would not have sufficient guidance on how to comply. For example, what if physician practices do not have a website? If practices are owned by hospitals, does the information have to be present on the practice website, the hospital website, or both?

A comprehensive regulatory scheme already requires the reporting by health care providers of health information breaches, including:

1. **Vermont Security Beach Notice Act, 9 V.S.A. § 2430 and 2435**
   a. **To what entities does the law apply:**
   The definition is very broad and includes any "data collector:" "Data collector" may include the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose,

134 MAIN STREET • P.O. BOX 1457 • MONTPELIER, VERMONT 05601-1457
TEL.: 802-223-7898 • 800-640-8767 • FAX: 802-223-1201

whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

b. Definition of "breach":

9 VSA § 2430: "Security breach" means unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by the data collector.

(5)(A) "Personally identifiable information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: (i) Social Security number; (ii) motor vehicle operator's license number or nondriver identification card number; (iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; (iv) account passwords or personal identification numbers or other access codes for a financial account.

c. What happens if there is a breach:

Within 14 business days of discovery of the breach: entity must give Preliminary Notice to the Attorney General

In the most expedient time possible and without unreasonable delay, but not later than 45 calendar days over the discovery or notification of the breach: consumer notice. The notice will be posted on the Attorney General's website. (See list of notices: http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-security-breaches.php)

When notice to consumers is sent: a copy of the Consumer Notice and the number of Vermont Consumers affected to the Attorney General

For more information,
see http://ago.vermont.gov/assets/files/Security%20Breach%20Guidance.pdf

2. HIPAA Breach Notification Rules

HHS issued regulations requiring health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached. These "breach notification" regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

a. Definition of "breach":

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An

impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of four factors.

b. **Notification requirements**:

To the individual: covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.

To the media: Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals are required to provide notice to prominent media outlets serving the State or jurisdiction.

Notice to the Secretary In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

For more information, see http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Thank you for your consideration of these issues and please feel free to contact us if you have further questions or need any additional information.