EXISTING MECHANISMS FOR ADDRESSING HIPAA BREACHES

S. 155, SECTION 1

Witnesses have testified that S. 155, Section 1 should be amended to allow patients who believe that their health information was disclosed inappropriately to file a law suit in Vermont Superior Court. Such a private right of action for HIPAA violations is unnecessary as a number of avenues already exist to provide redress to patients who believe their health information has been disclosed in violation of HIPAA. They include:

1. ***Private civil suits:***

As a comprehensive regulatory scheme, HIPAA creates the standard of care for how health care professionals and entities should maintain the privacy of health care information. As such, breaches of HIPAA can provide the basis for a professional negligence suit or other state law cause of action such as invasion of privacy or infliction of emotional distress. According to attorneys in private practices whom we have consulted, Vermonters are currently bringing private suits and regularly obtaining settlements. The proposed addition of a private right of action specifically for HIPAA violations along with automatic damages and attorneys fees would create an incentive to bring lawsuits with little or no merit.

2. ***Unprofessional Conduct Complaints***:

The professional boards that license health care providers consider breaches of HIPAA and Vermont's law on health care confidentiality (18 VSA § 1852 (7)) to be unprofessional conduct. For example, see 26 VSA § 1354 (24) and (27) for physicians. The Board of Medical Practice will receive and investigate complaints from patients regarding improper handling of their medical records and has issued orders based on HIPAA violations.

3. ***United States Health and Human Services, Office of Civil Rights Enforcement***

As explained in VMS's testimony to the House Judiciary Committee on April 14th, the Office of Civil Rights is tasked with investigating complaints of HIPAA violations. OCR can impose civil money or criminal penalties on health care providers for violations, ranging from a minimum of a $100 civil fine to $250,000 and imprisonment. Patients can file complaints with OCR in writing by mail, fax, e-mail, or via the Online OCR Complaint Portal. The OCR maintains a comprehensive website describing the complaint process for patients: http://www.hhs.gov/hipaa/filing-a-complaint. Health care providers are required to inform all patients of their right to file a complaint with OCR in the Notice of Privacy Practice that they distribute to patients.

4. ***State Attorney General Enforcement:***

In 2009 state attorney generals were granted enforcement authority for HIPAA violations. States can bring civil actions on behalf of state residents and obtain damages on behalf of states residents or enjoin further violations of HIPAA. Patients can file complaints with the Vermont Consumer Assistance Program by email, fax, mail or an online form, or they can contact the Attorney General's office directly. See https://www.uvm.edu/consumer/?Page=complaint.html. The Vermont Attorney General's office has confirmed that they follow up on HIPAA complaints received.

Adding additional avenues for legal action against physicians, their practices or employees will require them to put up a defense in court, create a strong disincentive against information-sharing allowed under HIPAA, and make it more challenging to attract physicians to practice in Vermont.

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

Witnesses also suggested the creation of a reporting requirement for privacy breaches. A comprehensive regulatory scheme already requires the reporting by health care providers of health information breaches including:

1. Vermont Security Beach Notification

Vermont's Security Breach Notice Act, 9 V.S.A. § 2430 and 2435, requires businesses – including health care entities - to notify the Attorney General and consumers in the event of a security breach of personal information. Businesses are required to notify the Office of the Attorney General within 14 days of discovering a breach and notification to consumers must be sent as soon as possible and no later than 45 days after discovery of the breach.

2. HIPAA Breach Notification Rules

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary of Health and Human Services, and, in certain circumstances, to the media.

These regulations define the information protected, breaches and other crucial terms. The language proposed will add confusion to a complex regulatory arena.