Vermont Association of Area Agencies on Aging
advocacy | action | answers

Contact
Mary Hayden, Executive Director
27 Main St., Suite 14
Montpelier, VT 05602
maryh@vermont4a.org
(802) 225-6210

S.71 *An act relating to consumer data privacy and online surveillance*
Senate Committee on Institutions
March 12, 2025

The Vermont Association of Area Agencies on Aging (V4A), on behalf of Vermont's five Area Agencies on Aging (AAAs), submits the following information and **respectfully asks this Committee to support S.93** (*An act relating to relating to data privacy*) **instead of S.71** (*An act relating to consumer data privacy and online surveillance*).

Area Agencies on Aging

Vermont's five Area Agencies on Aging (AAAs) coordinate and provide free supports that enable Vermonters and individuals with disabilities to meet their health-related social needs and age with dignity, both at home and in their communities.

Our services include: case management (long-term care coordination); home-delivered meals ("Meals on Wheels"); community meals; caregiver support; information and assistance helplines; Medicare counseling and education; wellness activities and programs; and, outreach and application assistance for benefits, such as VPharm, Medicare low-income savings, housing, fuel assistance, and 3SquaresVT.

Many of our services are funded by Medicaid and the federal Older Americans Act (OAA). We also receive state and federal grants funded and regulated by agencies such as the Department of Disabilities, Aging, and Independent Living (DAIL), Department of Vermont Health Access (DVHA), Department for Children and Families (DCF), Centers for Medicare and Medicaid Services (CMS), Administration for Community Living (ACL), Department of Veterans Affairs (VA), and AmeriCorps. All of these funders and regulators require us to maintain the confidentiality of client data.

HIPAA Privacy & Security

As some of our services are funded by Medicaid, the AAAs qualify as covered entities under the Health Insurance Portability & Accountability Act (HIPAA). Some of our services (such as Meals

on Wheels) do not qualify as healthcare services, even though these services create and store both Protected Health Information (PHI) and sensitive, non-health-related client data. The HIPAA regulations allow agencies such as ours, which provide both healthcare and non-healthcare services, to self-designate as non-hybrid entities. By self-designating as non-hybrid entities, we are able to apply the HIPAA privacy and security standards to all PHI, regardless of the program creating and storing the PHI. And given that all of our funders and regulators require us to maintain the confidentiality of client data, applying the HIPAA standard to all client data (including client data that isn't health-related) allows us to minimize compliance costs and administrative burden while still protecting client data to the stringent standards required under HIPAA.

AAAs' Existing Privacy & Security Practices

As non-hybrid covered entities under HIPAA, the AAAs must comply with the HIPAA Privacy and Security Rules with respect to all Protected Health Information (PHI) we create, store, and transmit. In the interest of protecting all client data, and to minimize compliance costs and administrative burden, we apply these same standards to client data that isn't health-related, as well:

(1) We've created HIPAA-compliant Notices of Privacy Practices (NPPs) that inform our clients of our practices with respect to their health information (e.g., how we use and disclose it).

(2) Our clients may request copies of their records, direct us to send their records to a third party (such as another service provider), request amendments to their records, and ask for an accounting of the third parties to whom we've sent their records.

(3) Our new staff members receive training in privacy and security shortly after hire. Our existing staff members receive ongoing training throughout the year.

(4) We audit and monitor our information systems, conduct risk assessments, and respond to all privacy and security concerns.

(5) We've established privacy and security policies and procedures.

(6) We use information systems only after they've been vetted for compliance with privacy and security standards and best practices.

S.71's Unnecessary Burden

As detailed above, the AAAs are already in the practice of applying the HIPAA Privacy and Security Rules to all client data, regardless of whether the data is health-related or not. Our current approach offers many benefits: we train our staff to a single standard, communicate a single set

of standards and practices to our clients and regulators, and avoid the unnecessary burden of precisely differentiating client health data from client data that isn't health-related.

If S.71 is passed, as written, we will have to discontinue our current approach and adopt an approach that is unnecessarily burdensome and costly. Because S.71 exempts only Protected Health Information (PHI) – but does not simultaneously exempt the non-health-related client data that we create and maintain – we will have to hold these two types of personal data to different standards.

Under S.71, we will have to precisely delineate PHI from non-PHI and then apply the HIPAA standards to the PHI (client health data) and the S.71 standards to the non-PHI (client non-health-related data). Most AAAs do not have the resources to hire the legal and compliance professionals that would be needed to assist with such an effort. It is also likely that holding our client data to two different standards will lead to significant confusion for our staff and clients. For example, many of our clients will need to receive two sets of privacy policies – a HIPAA-compliant Notice of Privacy Practices (applying to their health information) and a S.71-compliant privacy policy (applying to their non-health-related information).

Why S.93 is Better for the AAAs

S.93 alleviates the burden that S.71, as written, would place on the AAAs by following the lead of the majority of states that have already passed comprehensive privacy laws: S.93 fully exempts, at the entity level, all HIPAA covered entities and non-profit organizations.

If S.93 is passed instead of S.71, the AAAs will be able continue our HIPAA-compliant privacy and security practices for all client data, while continuing to focus on the important work that we do in every corner of our state.

Thank you for the opportunity to submit V4A's testimony concerning S.71 and S.93. Please let me know if you have any questions.

Mary Hayden, Executive Director
Vermont Association of Area Agencies in Aging (V4A)
maryh@vermont4a.org
(802)225-6210