To House Committee on Commerce & Economic Development

From Bobby Leonard, Compliance & Privacy Officer (Age Well, Inc.)

Date April 28, 2026

Re: S. 71 An act relating to consumer data privacy and online surveillance

The Vermont Aging Network Consortium, Inc. (VANC) is a member nonprofit organization, comprised of Vermont's five Area Agencies on Aging (AAAs). The AAAs are nonprofit organizations designated under the Older Americans Act to serve older Vermonters, individuals with physical disabilities, and their caregivers in every region of the state. Together, the AAAs deliver essential community-based services, including case management, care coordination, nutrition and meal programs, volunteer services, caregiver support, health insurance counseling and education, wellness activities, information assistance and referrals, and application assistance for benefit programs. Each year, the AAAs serve tens of thousands of Vermonters, many with complex health, functional, and social needs.

All five AAAs are non-hybrid HIPAA-covered entities. We already operate under one of the most comprehensive privacy frameworks in federal law, and we protect client information accordingly. Much of the data we collect must also be retained to meet Medicaid requirements, federal and state grant conditions, audit standards, and program-integrity obligations.

Existing regulatory obligations under HIPAA

As HIPAA-covered entities, the Area Agencies on Aging already operate under extensive, enforceable federal privacy requirements governing how client information is collected, used, disclosed, safeguarded, and retained.

These obligations include:

- limiting use and disclosure of Protected Health Information to permitted purposes related to care and operations;
- implementing administrative, technical, and physical safeguards;
- providing clients with a Notice of Privacy Practices explaining how their information is used and what rights they have;
- responding to client requests for access and correction within established timeframes;

- training staff on privacy and confidentiality requirements; and
- being subject to audits, enforcement actions, and penalties for non-compliance.

Importantly, in practice the AAAs do not draw sharp internal distinctions between "PHI" and other types of client information when it comes to privacy protections. Although HIPAA's definition of Protected Health Information is specific, the AAAs apply HIPAA-level confidentiality, security, and disclosure requirements to all client data because clients experience this information as a single record and expect it to be protected consistently.

HIPAA is specifically designed for health and human-services settings, balancing strong privacy protections with the need for continuity of care, service coordination, accountability, and program oversight.

Draft 2.3 does not replace this framework. Instead, it layers a general consumer-privacy statute on top of an environment where client data is already uniformly protected under HIPAA-based practices, even when the data is not legally PHI.

How AAA records reflect real lives, not discrete data categories

In practice, the AAAs do not document services in discrete data categories. We document people's lives as they are lived—with health concerns, functional needs, social circumstances, and personal context all intertwined.

A single conversation with a client may naturally include:

- information about health or mobility,
- details about what help is needed to live safely day to day,
- social or household circumstances affecting well-being, and
- personal preferences that shape how services should be delivered.

These elements are not separable during service delivery. They appear together in the same notes, the same conversations, and often the same sentences, because that is how effective, person-centered support works.

From the client's perspective, this is all simply "my record"—the information that explains who they are, what they need, and how services are helping. From a caregiver's perspective, it is the context that allows them to understand and support a loved one. From a staff perspective, it is the minimal, necessary context required to provide appropriate and effective services.

Draft 2.3, however, evaluates records through a different lens. Once the statute applies, it regulates personal data at the level of individual data elements, not at the level of the service record as a whole. This means that within a single AAA note:

- some information may fall within an exemption, while
- other information—created in the same interaction for the same client—may remain fully regulated under the consumer-privacy provisions of the bill.

This record-level fragmentation is not how AAA services are designed or delivered. The following examples illustrate how these distinctions emerge in everyday AAA work and why they create staff burden and client confusion without improving privacy protection.

Example 1: A routine request for access and deletion

A client contacts an Area Agency on Aging and says:

"I want a copy of everything you have about me, and I want some of it deleted."

Today, staff know how to respond under HIPAA. The client is given timely access to their record, and staff explain—clearly and consistently—why service records generally must be retained to support care coordination, Medicaid compliance, audits, and legal accountability.

Under Draft 2.3, this same request becomes more complicated. Any non-exempt personal data in the client's file is now subject to a statutory deletion right unless retention is required by law. That means staff must review records, prepare a written denial explaining why deletion cannot occur, and provide information about appeal rights.

From the client's perspective, this is confusing. The law grants a deletion right that, in practice, often must be denied. Even when staff handle the request correctly, the experience feels inconsistent and frustrating, and it places staff in the position of explaining why different rules apply to what the client experiences as a single record.

Example 2: A single service-coordination note

A case manager documents an ordinary interaction in a client's file:

"Client reports difficulty standing for more than ten minutes; needs transportation to clinic; prefers morning appointments; daughter is backup contact."

This single sentence includes several types of information:

- health-related observations,

- functional support needs,
- personal preferences, and
- caregiver contact information.

Some of this information may qualify as Protected Health Information under HIPAA. Other information, such as preferences and caregiver context, are personal data but often not PHI.

Under Draft 2.3, staff must treat these data elements differently, even though they were created together in the same interaction for the same purpose.

For compliance purposes, staff must be prepared to explain which parts of the note are exempt and which are fully regulated under the consumer-privacy statute. For the client, however, this distinction is invisible. They reasonably experience this as one unified service record. What was once straightforward documentation becomes legally fragmented.

Consequences if Draft 2.3 becomes law (for AAAs and the Vermonters we serve)

If Draft 2.3 becomes law, the AAAs' experience will not be a dramatic change in how we protect client information; we already protect client data to HIPAA standards. The change will be in the administrative burden and the client experience created by applying a second privacy framework to non-PHI personal data embedded throughout ordinary service records.

For the AAAs and our staff, the most immediate impacts will be:

- **Time diverted from services to compliance**: increased staff time spent triaging requests, determining what is exempt versus covered, preparing written denials, and managing appeals.
- **More hesitation in documentation and coordination**: staff will feel pressure to sanitize notes or limit contextual detail, reducing effectiveness of service delivery and care coordination.
- **Increased reliance on legal counsel and compliance services**: limited nonprofit resources will be redirected to legal review, policy development, staff training, and ongoing compliance support to manage new consumer-privacy obligations, reducing resources available for direct services.

For clients and caregivers, the most immediate impacts will be:

- **Confusion about rights**: clients will reasonably believe they have rights—especially deletion—that frequently must be denied due to legal retention requirements, creating frustration and mistrust.

- **Fragmented explanations for a single record**: clients experience their file as “my record,” but will receive different answers depending on whether specific elements are PHI or non-PHI personal data.
- **More appeals and complaints**: confusion and perceived inconsistency will lead to more follow-up requests, appeals, and complaints, making the client experience more adversarial and further consuming staff capacity.

In short, Draft 2.3 would impose a new layer of process on top of an already regulated environment, producing more friction, more confusion, and less staff time for direct services, without meaningfully improving privacy protections beyond what already exists under HIPAA-based practices.

Request to advance S.71 as passed by the Senate

For the reasons described above, VANC and the AAAs respectfully urge the Committee to advance S.71 as it was passed by the Senate, without adopting Draft 2.3.

The Senate-passed version of S.71 takes a clear, structurally sound approach. It recognizes that HIPAA-regulated entities already operate under comprehensive, enforceable privacy frameworks that are specifically designed for health and human-services settings. By regulating at the entity level, rather than attempting to govern individual data elements within client service records, the Senate version avoids the operational, client-experience, and resource-limitation problems described in this testimony.