ataACTION
Telehealth Policy to Transform Healthcare

December 8, 2025

The Honorable Aaron Michlewitz
Chair, House Committee on Ways and Means
Massachusetts House of Representatives
State House, Room 243
Boston, MA 02133

RE: ATA Action Comments Regarding Massachusetts S. 2619

Dear Chair Michlewitz,

On behalf of ATA Action, I am submitting the following comments regarding S. 2619, *An Act Establishing the Massachusetts Data Privacy Act.* We commend the Legislature's commitment to enhancing consumer privacy protections. However, several provisions in the Senate-passed version may unintentionally restrict responsible uses of health data, impede the delivery of telehealth services, and create operational challenges for healthcare providers and digital health companies.

ATA Action, the American Telemedicine Association's affiliated trade association focused on advocacy, advances policy to ensure all individuals have permanent access to telehealth services across the care continuum. ATA Action recognizes that telehealth and virtual care have the potential to truly transform the health care delivery system – by improving patient outcomes, enhancing safety and effectiveness of care, addressing health disparities, and reducing costs – if only allowed to flourish.

ATA Action has several targeted concerns regarding the sensitive data (including health data) privacy provisions of the legislation, which we believe could create conflicting obligations for telehealth providers and introduce unnecessary compliance uncertainty. Thankfully, Massachusetts can look to neighboring Connecticut for guidance, as the *Connecticut Data Privacy Act* (CTDPA) includes several balanced provisions that we recommend as alternatives to the current language. Specifically, ATA Action offers the following recommendations:

Amend the provisions regarding "strict" processing of sensitive data to better align with HIPAA: As Section 5(a)(iii) is currently drafted, an entity would be only allowed to collect, process, or transfer sensitive data when it is "strictly necessary" to provide the specific product or service requested—absent only narrow exceptions. This overly rigid framework would prohibit common, beneficial, and low-risk activities that require processing of sensitive data (broadly defined). For example, healthcare entities and digital health platforms would be prohibited (even if they had authorization) from activities such as informing patients about new clinical offerings, using the data to improve product and service offerings, improving customer support operations, or training and improving new and developing technologies. In effect, this will deteriorate the range and quality of health services, products and technologies offered to Bay Staters.

In contrast, under the HIPAA Privacy Rule, covered entities—and, in certain cases, their business associates—may perform these same activities using protected health information *even without* obtaining separate authorization. This inconsistency creates divergent rights for Massachusetts consumers and

unequal compliance burdens on entities doing business in the Commonwealth based solely on HIPAA exempt status.

We respectfully urge the General Court to amend Section 5(a)(iii) to remove the "strictly necessary" qualification and instead incorporate provisions similar to the CTDPA, which more appropriately balances consumer protection with operational feasibility, including strong protections for both sensitive and consumer health data. The proposed amendments below require controllers to avoid processing, collecting or transferring sensitive data without affirmative consent but does not impose an unworkable "strict necessity" standard that could unintentionally restrict legitimate, privacy-protective uses of data in telehealth and health technology applications.

> (iii) not collect, process or transfer sensitive data concerning a consumer *without obtaining the consumer's affirmative consent, or, in the case of collection or processing of sensitive data concerning a known child, without processing such data in accordance with Children's Online Privacy Protection Act, 15 USC 6501 et seq;* ~~except when such collection, processing or transfer is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;~~

By adopting these amendments and removing the "strictly necessary" qualification, this Act will better align with HIPAA and allow regulated health information to be used for treatment, payment, and health-care-operations purposes. This approach preserves strong consumer protection while maintaining the flexibility necessary for innovation, patient communication, and high-quality care delivery.

Revise Provisions on Sale of Data to be Consistent with HIPAA:
Section 5(a)(iv) establishs that a controller is prohibited from selling sensitive data, with no consideration of consumers' explicit authorization. However, under the HIPAA Privacy Rule, individuals currently can—*and do*—authorize entities to disclose their protected health information ("PHI") for marketing, including in instances where an entity discloses the individual's PHI to a third party in exchange for a "direct or indirect remuneration."[1] For example, an individual may authorize their provider to disclose their PHI to a pharmaceutical firm so that the individual receives discounts on medications, even where the individual provider receives remuneration from the pharmaceutical firm.

ATA Action believes the current HIPAA rules provide detailed and appropriate protection for the confidentiality of protected health information, as these rules have been a fixture in our healthcare system for more than two decades. We are concerned that the total prohibition on the sale of sensitive data contemplated in this Act would create inconsistent and conflicting obligations on HIPAA entities when the "sensitive data" at issue would not constitute PHI that is exempt from the Act. Furthermore, to the extent that PHI is exempt from the sale prohibition, this Act would then afford differing rights to Massachusetts consumers as to the sale of their data and unequal burdens on entities based solely on being subject to HIPAA.

To be certain, ATA Action shares the sponsors' intent to protect sensitive data and our Data Privacy Principles emphasize that sensitive data should always require explicit disclosure to, and consent from, the consumer. We respectfully request the provision regarding the sale of sensitive data be amended to

[1] Summary of HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

ata ACTION
Telehealth Policy to Transform Healthcare

better align with HIPAA and other states such as Connecticut, Delaware and Rhode Island (which all require opt-in consent to process sensitive data, including for purposes of sale) such that:

Section 5(a)(iv)

"a controller shall… not sell sensitive data *without obtaining the consumer's affirmative consent*."

Include exceptions for data use practices that are consistent with HIPAA:
We support the language of Section 9(a) of the Act which permits controllers to conduct a specific number of data processing activities. We encourage the General Court to also explicitly make clear that controllers may undertake internal research and development, product recalls, internal operations and other standard business practices that comply with existing health privacy rules. This ensures that HIPAA-covered entities and their partners can continue essential innovation and patient safety activities without unintended legal uncertainty**.** We believe the following amendments, incorporated from CTDPA, will satisfy these important considerations without undermining the intent of the Act:

Section (9)(a) …

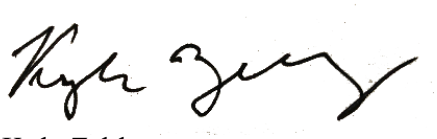
(xvi) *to collect, use or retain data for internal use to* perform internal operations ~~from data collected in accordance with this section that~~ that are reasonably aligned with the expectation of the consumer based on the consumer's existing relationship with the controller…

(xviii) *) Conduct internal research to develop, improve or repair products, services or technology.*

ATA Action hopes that the General Court will embrace these changes to simultaneously ensure patient data is effectively protected while not placing undue burdens on providers. We believe that our proposed amendments reflect a fair balance between these two significant public policy goals.

Thank you for your support of telehealth. We encourage you and your colleagues to consider amendments to this bill to ensure easy and efficient access to high-quality health care services in Massachusetts. Please do not hesitate to let us know how we can be helpful to your efforts to advance common-sense telemedicine policy. If you have any questions or would like to discuss the telemedicine industry's perspective further, please contact me at kzebley@ataaction.org.

Kind regards,



Kyle Zebley
Executive Director
ATA Action