ata ACTION
Telehealth Policy to Transform Healthcare

January 11, 2024

Hon. Steven Otis
Chairman, Assembly Committee on Science & Technology
Assembly Member, District 91
LOB 739
Albany, NY 12248
OtisS@nyassembly.gov

RE: ATA ACTION COMMENTS OPPOSING ASSEMBLY BILL 4983--B

Dear Chairman Otis and members of the Assembly Committee on Science & Technology**,**

On behalf of ATA Action, I am writing you to express concerns on Assembly Bill 4983--B, the New York Health Information Privacy Act, and to encourage the Assembly to work with stakeholders on what is a very complex issue with possible unintended consequences.

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 supports efforts to ensure telehealth practices meet standards for patient safety and data privacy, while advancing access to care and awareness of telehealth practices. In light of the advancement of privacy legislation in many states across the country directly or indirectly affecting telehealth practice, ATA Action has published its Health Data Privacy Principles (attached) to aid legislators in crafting legislation that supports both secure data practices and ensures patient access to care. ATA Action hopes these policy principles are helpful in crafting forward-thinking and thoughtful privacy legislation in New York.

ATA Action has several concerns that A4983 ("the Act") runs counter to sound data privacy policy and puts undue burdens on telehealth providers due to its complexity and undefined breadth. Specifically, ATA Action makes the following recommendations:

Legislators should seek uniform privacy laws consistent across states and industries: As states adopt privacy laws across the nation, efforts to establish uniformity with existing federal and other state standards would reduce both complexity and costs regarding compliance, as well as confusion for consumers. Unfortunately, the Act at hand is both specific only to healthcare and creates uneven burdens on providers relative to federal laws (discussed below). Instead, ATA Action encourages legislators to take an approach that mirrors Virginia (see the Virginia Consumer Data Protection Act[1]) and Connecticut (see the Connecticut Consumer Data Privacy and Online Monitoring Act[2]). As A4983--B continues to

[1] Virginia Consumer Data Protection Act, VA Code Ann. § 59.1-575 *et seq*., https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.
[2] Connecticut Consumer Data Privacy and Online Monitoring Act, Conn. Gen. Stat. § 42-515 *et seq*., https://www.cga.ct.gov/current/pub/chap_743jj.htm.

work through the legislative process, we hope this Committee and the Vermont legislature will strive for uniformity with these existing state regulatory frameworks and avoid burdensome requirements that would be specific to New York.

A4983-B is inconsistent with HIPAA despite the bill's stated intent: The synopsis of A4983-B notes that New York residents have the misimpression that HIPAA protects them anytime they share health information and that this legislation intends to afford privacy protections where HIPAA would not apply. ATA Action supports this intent and strongly agrees "state consumer privacy laws should be consistent with and not exceed HIPAA's standards to the greatest extent possible."

However, we echo the concerns other stakeholders have expressed that this Act imposes obligations and requirements that exceed HIPAA and other existing state and federal regulatory frameworks, creating significant uncertainty about compliance. The lack of clarity is particularly troubling as our organization represents both HIPAA and non-HIPAA covered entities, who nonetheless share a commitment to protect the confidentiality of patient's personal information. Some of examples of how this legislation is inconsistent with and exceeds HIPAA include:

> ***A4983--B prohibits marketing activities permitted under HIPAA:*** Under the proposed Act, a regulated entity would need a specific consent to both collect and use a consumer's data for any purpose other than to provide the product or service that the consumer requested. This would, for example, prohibit a regulated entity from sending communications about its additional products or services to the consumer. However, a HIPAA-covered entity – and in some situations their contracted business associates – could engage in that same activity with the consumer's HIPAA protected health information without any need for specific consent from the consumer under the HIPAA Privacy Rule.[3] This inconsistency not only undermines the stated intent of the Act, it would afford differing rights to New York consumers and unequal burdens on entities based solely on being subject to HIPAA. We suggest aligning the permitted uses and disclosures of the Act, at a minimum, with the HIPAA Privacy Rule, including that consumer health data may be used for purposes of treatment, payment, and health care operations.
>
> ***A4983--B proposes a unique burden that consumers must wait 24 hours before providing authorization:*** Unlike HIPAA, Section 1102(2)(a)(ii) states that a request for a consumer's valid authorization can only be made at least twenty-four hours after the consumer signs up for, or first uses the product or services. As an initial matter, increasing the steps in a sign-up process to a multi-day event will risk a significant drop off in consumer retention rates and increases the administrative burden on the regulated entity. But more importantly, this rule would also arbitrarily contravene the intent of A4983--B, which in part is meant to ensure consumers have adequate notice about a regulated entity's data practices *when the consumer begins to provide their personal health information to that entity*, not 24-hours after. Consumers more-likely-than-not appreciate receiving this information at the beginning of a sign-up process (as they would at a physician office), not after they have already provided information to the regulated entity.
>
> ***A4983--B has an unprecedented requirement that consumer authorization expires at 1 year:*** The Act states that an authorization must have an expiration date and that it must be within a year

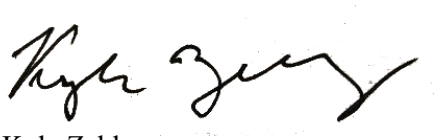
[3] *Marketing*, U.S. Dept. of Health and Human Servs. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html.

of signing. ATA Action is unaware of any state or federal requirement that mandates a consumer's authorization expires after a year, even if the parties have agreed otherwise. For example, a HIPAA authorization remains valid until it expires or is revoked by the individual. We recommend the Act align with HIPAA and not prescribe limits on the authorization.

A4983--B informed consent requirements and restrictions to process health data are overly burdensome and impractical: A4983--B intends to ensure that regulated entities need "separate consent" to sell any health information to third parties. While ATA Action agrees with requiring prior authorization for sale of health data, this Act goes much further and requires authorization beyond sale and to any processing for which there is not an exemption. ATA Action has concerns that requiring multiple authorizations—rather than a single authorization—will lead to consent fatigue and potentially lead to confusion for users who are simply trying to access a healthcare service. Further, Sections 1102(2)(b)(vi) and 1102(2)(g) would compel regulated entities to provide services to consumers when those consumers opt-out of providing a valid authorization for particular uses of their health data. ATA Action has concern about forcing healthcare entities and other businesses to provide services to consumers when those consumers freely reject the terms offered by such businesses. We encourage the Legislature to strike these sections as they may have the unfortunate effect of significantly reducing the incentive for innovative digital health applications to offer free or reduced-price services and ultimately restricting the options available to all New York consumers.

Please see the attached Privacy Principles for greater detail on ATA Action's data privacy policy positions and do not hesitate to let us know how we can be helpful to your efforts to advance common-sense telehealth policy. If you have any questions or would like to discuss the telehealth industry's perspectives further, please contact me at kzebley@ataaction.org.

Kind regards,



Kyle Zebley
Executive Director
ATA Action