May 20, 2026

New York Assembly Committee on Codes
Room 630, Legislative Office Building
198 State Street
Albany, NY 12248

Re: A 10357 - "Providing for the Protection of Health Information" (Oppose)

Dear Chair Dinowitz and Members of the Assembly Committee on Codes

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose A 10357. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1]

CCIA shares the Legislature's commitment to ensuring New York residents' healthcare information. However, A 10357 carries many of the same concerns CCIA highlighted regarding its 2025 counterpart.[2] The bill creates an unworkable regulatory framework that would stifle innovation, jeopardize privacy, and burden both consumers and businesses. Specifically, the bill presents the following concerns:

The bill's key definitions are overbroad.

Many of A 10357's key terms are defined more broadly than necessary, encompassing routine transactions as well as sensitive health data. For instance, the bill defines "Regulated health information" as personally identifiable information that "is collected or processed in connection with an identified or identifiable individual's past, present, or future physical or mental health status." This definition could extend to routine purchases of any product connected to a consumer's physical health, such as sunscreen, vitamins, or shoe inserts. Accordingly, the bill risks extending detailed, costly compliance requirements to any vendor carrying these routine products, even if the vendor provides no actual healthcare. CCIA recommends instead limiting this term to only cover data used to identify an individual's health status, as states such as Connecticut and Nevada have done.[3]

Likewise, the bill prohibits regulated entities from sharing any "regulated health information for monetary or other valuable consideration," without creating an exception for regulated entities'

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

[2] *See* Megan Stokes, *NY's Health Privacy Bill Creates More Problems than it Solves, Could Make it Harder to Get Care*, Rochester Bus. J. (May 9, 2025), https://rbj.net/2025/05/09/ny-health-privacy-bill-opinion/.

[3] *See, e.g.*, Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515(9) (2023) (defining "consumer health data" as "personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis or to obtain information about a consumer's health status"); Security and Privacy of Consumer Health Data, Nev. Rev. Stat. § 603A.430 (2023) (defining "consumer health data" as personally identifiable information linked or reasonably capable of being linked to a consumer that a regulated entity uses to identify the consumer's past, present, or future health status).

data processors. Many companies contract with third parties to securely process data on their behalf, and the bill's current language prohibits this practice. This requirement would severely limit competition without improving user privacy. CCIA instead recommends expressly exempting regulated entities' data processors from this prohibition, following Connecticut and New Jersey's example.[4]

The bill's requirements undermine privacy.

A 10357 covers entities that serve individuals who are "physically present in New York". This provision therefore effectively requires regulated entities to track their users' locations, thus undermining the privacy of the very population the bill is designed to protect. Many individuals commute between New York and surrounding states daily for work, and different privacy laws would apply to these individuals at different times of day. Forcing regulated entities to collect information they would not collect otherwise will not protect consumers' privacy.

The bill's data processing limitation puts New York businesses at a competitive disadvantage.

Absent a federal privacy framework, interoperability between state privacy laws is crucial to avoid placing a difficult, confusing, and costly compliance burden on businesses. However, A 10357 disadvantages New York businesses by holding them to a stricter data minimization standard than their out-of-state counterparts. Most state privacy laws limit data processing to what is "reasonably necessary" for the disclosed purposes for which the personal data is processed.[5] However, A 10357 instead prohibits regulated entities from processing an individual's personal data unless "strictly necessary" to provide "a specific product, feature, or service requested by such individual", with narrow and limited exceptions.

Determining whether a product or service can be provided without processing a given piece of data will likely require significant technical expertise, even for businesses without technically complex operations. This regulation is likely to create barriers to entry in many industries, and deter out-of-state businesses from expanding into New York. CCIA therefore recommends substituting the standard limitation, under which regulated entities may process data that is reasonably necessary for a disclosed purpose.

The bill creates unnecessary compliance burdens that do not serve consumers.

A 10357 requires regulated entities to repeatedly request consent for similar transactions, a requirement which could be simplified considerably without loss of privacy. The bill requires regulated entities to make authorization requests " separately from any other transaction or part of a transaction." Since the bill does not define "transaction" or state when it is divided into "parts," it is unclear how often consent must be requested. The bill could be interpreted,

[4] *See* Conn. Gen. Stat. § 42-515(37); N.J. Rev. Stat. 56:8-166.4(1) (2025) (each excluding "the disclosure of personal data to a processor that processes the personal data on behalf of the controller" from the definition of "Sale").
[5] *See, e.g.*, Conn. Gen. Stat. § 42-520(a)(1) (2024), https://www.cga.ct.gov/2024/sup/chap_743jj.htm; Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.101(a)(1) (West 2024), https://statutes.capitol.texas.gov/?tab=1&code=BC&chapter=BC.541&artSec=.

for instance, to require consent for each individual healthcare-related item purchased in a pharmacy, such as band-aids or dietary supplements. Each of these consent requests would require large quantities of information, including categories of recipients, processing purposes, monetary consideration, and other lengthy disclosures. Endless repetitions of such authorization requests are unlikely to meaningfully inform users. Instead, this provision risks contributing to "consent fatigue," a phenomenon widely observed in the European Union following implementation of the General Data Protection Regulation, where frequent and repetitive notices lead users to disengage and reflexively accept terms without meaningful review.[6]

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as New York considers proposals related to technology policy.

Respectfully submitted,

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association

[6] Luis Montezuma, *How to avoid consent fatigue,* https://iapp.org/news/a/how-to-avoid-consent-fatigue, IAPP (Jan. 29, 2019). *See also*, *What Is Consent Fatigue and How to Combat It?,* Cookie Script, https://cookie-script.com/blog/consent-fatigue (May 17, 2024).