S.9269 (Krueger) / A.10357 (Rosenthal)

STAFF CONTACT : Chelsea Lemon | Senior Director of Government Affairs | 518.694.4462

BILL

S.9269 (Krueger) / A.10357 (Rosenthal)

SUBJECT

New York Health Information Privacy Act

DATE

May 12, 2026

OPPOSE

The Business Council has actively engaged in conversations on the New York Health Information Act (NYHIPA) and appreciates the continued dialogue between stakeholders, businesses, consumers and lawmakers. We continue to support the underlying intent of this legislation: protecting consumers' sensitive health information. Yet, we believe that the passage of reasonable consumer health data privacy laws must be done in a way that does not disrupt businesses or providers ability to improve consumer access to services and products, or misalign with privacy frameworks adopted by 20 other states.

Absent a federal privacy framework, states have stepped in to adopt their own privacy regimes. These structures provide meaningful consumer protections, reasonable business obligations, and consistent enforcement practices. Unfortunately, NYHIPA, even in its amended form, misaligns New York with practices adopted by other states, conflicts with HIPAA, the FTC and other laws, and will confuse consumers from understanding how to protect their sensitive health information.

Following Governor Hochul's veto of S.929/A.2141, The Business Council is encouraged by several of the amendments made to the bill that are reflected in S.9269/A.10357, including:

- **Removal of the 24-hour waiting period**
  - The amended NYHIPA removes the original bill's unique requirement that authorization be obtained at least 24 hours after a consumer creates an account or first interacts with the requested product or service. This mandatory delay would have grave ramifications for consumers looking to access time-sensitive health services or products or same-day delivery of over-the-counter medications.
- **Certain Exemptions**

    - The amended bill adds exemptions for employee and job applicant information, personal information subject to the Fair Credit Reporting Act, an entity-level exemption for business associates subject to the Health Insurance Portability and Accountability Act ("HIPAA"), information subject to FERPA, and exemptions for data collected as part of human subject research. However, it does not address all exemptions which were debated during discussions on the original bill.
- **Identity Verification**
    - The amended NYHIPA clarifies that a regulated entity must comply only with consumer rights requests that it can verify.
- **Removal of an excessively punitive penalty structure**
    - The amended bill removes language which would have allowed penalties to be assessed at up to 20% of revenue from New York consumers. It also includes a welcome requirement that courts must consider the severity of the violation and good faith compliance efforts when determining penalties. However, we maintain that $15,000 per violation is inconsistent with most other states privacy laws.

However, the bill retains NYHIPA's originally proposed structure and unprecedented approach to regulating consumer health data, creating an operationally unworkable framework and unintended consequences for consumers and businesses alike.

The Business Council remains committed to creating a privacy framework in New York that creates meaningful consumer protections that align with practices adopted in 20 other states, and like those of Colorado, New Jersey, Virginia, and Connecticut. However, NYHIPA deviates from these frameworks Therefore, The Business Council continues to strongly oppose the New York Health Information Act (S.9269 Krueger/A.10357 Rosenthal).

Definition of "Regulated Health Information"

The amended bill retains an expansive definition of Regulated Health Information (RHI) that covers data reasonably linkable to an individual and collected or processed "in connection with" their health status (NYHIPA § 1120(2)), but the phrase "in connection with" is ambiguous and overly broad, creating uncertainty about the scope of covered data and complicating compliance for regulated entities. This lack of clarity may

cause companies to over-notify or over-seek authorization, potentially overwhelming consumers and discouraging them from using beneficial products and services.

Compounding this issue, the bill's definition of "individual" to include persons acting in a “household” context further blur who the data subject is, generating uncertainty about whose rights apply, who may authorize processing, and when routine household-level interactions could trigger regulatory obligations.

We understand that the Legislature’s goal is to protect genuinely sensitive health data, and we support that goal. However, the current definition of RHI could sweep in a wide-ranging breadth of consumer products not intended to be captured, like a purchase of low-fat yogurt or athleisure apparel, or the viewing of swim technique videos online, simply because one could infer a health data point or status from those purchases or behaviors. The Business Council maintains that the definition of RHI should be amended to:

“Consumer health data means any personal data that a controller uses to identify a consumer’s physical or mental health condition or diagnosis and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.”

Definition of “Regulated Entities” and Definitional Overlap of “Regulated Entity,” “Service Provider” and “Third-Party”

The amended NYHIPA's definition of "regulated entity" raises significant concerns on multiple fronts. First, the bill applies more broadly than comparable consumer health privacy laws by covering any entity that controls the processing of RHI of individuals "physically present in New York," potentially capturing temporary visitors and commuters with only a tangential connection to the state. NYHIPA § 1120(4)(b). Rather than enhancing privacy, this broad geographic trigger may actually undermine it as companies that would not otherwise collect location data may be forced to do so simply to determine whether, and when, they fall within the bill's scope.

Compounding this problem, the bill's definitions of "Regulated Entity," "Service Provider," and "Third Party" overlap in ways that create confusion and impose unworkable obligations. While the bill acknowledges that a service provider "may also be a regulated entity depending upon the context," service providers by definition act on behalf of regulated entities and treating them as regulated entities is inconsistent

with Washington's My Health My Data (MHMD) and other comprehensive privacy statutes, none of which impose regulated entity-level duties on processors. Similarly, the bill's statement that a third party "may also be a regulated entity or service provider depending upon the context" is circular and leaves entities unable to clearly identify their role and corresponding obligations. NYHIPA § 1120(6). In practice, this framework would require backend vendors and service providers to obtain consumer consent from individuals they never interact with — an obligation that cannot be implemented at scale.

Definition of "Sell"

The bill's definition of "sell" is sweeping and notably lacks exceptions for two categories recognized by virtually every comparable privacy statute: disclosures to service providers and consumer-directed sharing. Unlike MHMD, Connecticut, and New Jersey law — all of which expressly exclude processor-level disclosures from the definition of "sell" — NYHIPA treats routine service-provider transfers as regulated sales, placing New York out of step with neighboring jurisdictions and forcing multi-state organizations to treat the same service-provider relationship as ordinary and permitted elsewhere but as a regulated transaction in New York. This inconsistency will require organizations to renegotiate contracts, manage conflicting obligations across states, and absorb a disproportionate compliance burden that will ultimately increase the cost of doing business and negatively impact consumer affordability.

Equally problematic, the definition's failure to exempt consumer-directed sharing means that ordinary operational data flows, like activities that consumers themselves initiate or request, could be swept in as a "sale," flooding routine transactions with unnecessary authorizations and alarming notices that will confuse rather than inform consumers and impede their ability to access services they actively seek.

"Strictly Necessary" Processing

NYHIPA's one-tier approach requires regulated entities to obtain valid authorization before processing RHI unless such processing is "strictly necessary" for a statutorily enumerated purpose — the most restrictive data minimization threshold available under any comparable law. *See NYHIPA § 1122.* The bill provides no clarification of what "strictly necessary" means in practice, introducing significant ambiguity and departing from states like Washington that apply the more workable "necessary" standard.

In practice, this threshold would require a telehealth platform to obtain standalone, detailed authorization before sending flu vaccination reminders, suggesting preventive screenings, or recommending wellness content — routine, consumer-beneficial activities that no other state privacy or consumer health data framework subjects to such requirements. Rather than strengthening privacy, this approach risks producing consent fatigue: consumers confronted with repeated, lengthy authorization requests will either abandon beneficial services or click through without reading, undermining the bill's own goals. Those who do engage may avoid seeking products, services, or health information altogether out of concern that their authorization could be traced back to them, or because the requirement to authorize access to sensitive services — such as contraception — feels unduly intrusive. More broadly, a strict necessity standard would impede routine operational functions that modern services depend on, including product development, security monitoring, fraud prevention, first-party advertising, and quality assurance — activities permitted under every other state privacy framework.

We urge the adoption of a "reasonably necessary" standard, which would provide consumers with meaningful privacy protections while preserving the proactive, consumer-beneficial data uses that support better health outcomes.

Overly Burdensome Consent Authorization Requirements

The bill's authorization requirements go far beyond any existing privacy or consumer health data statute and would impose obligations that are not operationally realistic. The mandate that refusing authorization "will not affect the individual's experience of using the regulated entity's products or services" conflicts with how consent systems work and would be impossible to implement in practice.

The amended bill also introduces additional prescriptive requirements that compound this burden, including a plain language and 12-point font mandate, a requirement to clearly state that processing is not strictly necessary, the ability for consumers to grant or withhold authorization for each individual category of processing, and a requirement to disclose any monetary or other valuable consideration a regulated entity may receive in connection with processing regulated health information, rather than limiting that disclosure to consideration received specifically for its sale.

Because NY HIPA defines "regulated health information" so broadly, organizations would need to present detailed, multi-element authorization notices constantly, covering disclosures, purposes, categories of

recipients, monetary consideration, expiration dates, revocation procedures, and access and deletion mechanisms. That frequency would desensitize consumers to genuinely sensitive data uses, undermine the value of meaningful consent, and create significant friction across routine interactions that do not involve health-related data in any conventional sense. This problem is further exacerbated by the bill's requirement that each request for authorization be made separate from any other "transaction," regardless of whether the two transactions may be related, which could force organizations to present consumers with multiple related yet slightly different authorization requests for related kinds of data processing, increasing consent fatigue and causing consumer confusion.

Collectively, these provisions create an overly burdensome compliance structure that exceeds other consent frameworks without delivering measurable improvements to consumer privacy. We also note that the amended bill retains the original 30-day timeframe for responding to consumer rights requests, which is shorter than the 45-day window provided under both MHMD and most state consumer privacy laws; this compressed timeline may incentivize the use of less robust verification methods, undermining the effectiveness of consumer rights and increasing the risk of unauthorized requests.

Exemptions

As mentioned above, some changes have been made to the amended bill’s exemption language. However, many of the exemptions debated during discussions on the bill remain absent from the amended bill’s text. The bill does not provide clear exemptions for organizations already heavily governed by federal privacy and security laws such as GLBA, SEC regulations, and other sector-specific frameworks. Without those exemptions, which are found in nearly all other states’ comprehensive and consumer health data privacy laws, entities subject to federal oversight would face overlapping and potentially conflicting obligations, creating parallel compliance regimes that cannot be reconciled in practice. The lack of clarity will force institutions to choose between violating federal requirements or violating NY HIPA, an outcome that makes legal compliance nearly impossible and exposes regulated sectors to significant operational and enforcement risks.

Enforcement

We have several significant concerns with the bill as currently drafted. The bill's six-year statute of limitations, triggered by the Attorney

General's "awareness" of a violation, is unnecessarily broad and subjects businesses to prolonged legal uncertainty; reducing the limitations period to three years would still ensure meaningful enforcement capacity while providing businesses with the regulatory predictability they need to confidently plan and invest. Second, the amended bill fails to explicitly foreclose a private right of action, instead retaining language stating that "[t]he remedies provided by this section shall be in addition to any other lawful remedy available," which introduces problematic ambiguity that could expose businesses to unanticipated litigation. Finally, the proposed penalty of $15,000 per violation is out of step with the majority of other state privacy laws; penalties should be capped at no more than $5,000 per violation to align with prevailing standards and avoid disproportionate liability.

Implementation Timeline

This amended bill contains a shortened effective date – from one year (in the original version S.929 of 2025) to six months after enactment. Given the complexity of the bill's authorization requirements and the breadth of its definitions, a six-month window is simply insufficient for regulated entities to audit data flows, build compliant systems, and retool consumer-facing interfaces. A more workable implementation timeline of two years from the date the legislation becomes law would give regulated entities the time needed to build durable, effective privacy programs while reducing the risk of service disruptions for New Yorkers.