HINMAN STRAUB PC
ATTORNEYS AT LAW

121 State Street
Albany, New York 12207-1693
Tel: 518-436-0751
Fax: 518-436-4751

June 2, 2026

RE: AN ACT amend the general business law, in relation to providing for the protection of health information

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

MEMORANDUM IN OPPOSITION

Submitted on behalf of the Blue Cross and Blue Shield Plans

The New York State Conference of Blue Cross and Blue Shield Plans opposes the enactment of this legislation, which would enact the New York Health Information Privacy Act to protect New Yorkers' health information. While this legislation is well-intentioned, the bill does not specifically exclude health plans and their business associates who are subject to separate federal and state statutory oversight, from compliance. Specifically, health plans are already subject to extensive federal and state privacy requirements, including Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This bill would increase unnecessarily administrative costs for plans that would be felt by employers and consumers though higher insurance premiums.

This bill would apply to regulated health information (including information reasonably linkable to a device and collected in connection with an individual's health status) in the possession of a related entity (meaning any entity that controls the processing of regulated health information of a person in New York or any entity located in New York). The bill prohibits the sale or processing of regulated health information outside of providing the specific product or service without expressed authorization. The authorization would be valid for no longer than one (1) year. The requirements would also apply to service providers (meaning entities that process regulated health information on behalf of a regulated entity), similar to how HIPAA applies to business associates. The bill would also authorize the Attorney General to bring an action when a person has violated the bill's provisions.

The Sponsor's Memorandum indicates that this bill is intended to apply to health data collected and used by entities that are not otherwise covered by HIPAA. For example, numerous apps exist to track fitness, sleep, mood or mental health, and nutrition. The entities providing these apps may not be required to comply with HIPAA, as they are not a health care provider, health plan, or

business associate subject to the HIPAA's requirements. However, as drafted, the bill sweeps in health plan activities that are already subject to extensive federal and state regulations on health information privacy, like HIPAA. The federal law limits a health plan's ability to use and share data by subjecting it to the privacy requirements in the HIPAA regulations, which applies to covered entities (e.g., health plans) and their business associates.

If applicable to health plans, this bill contains certain provisions that are inconsistent with HIPAA. For example, this bill would prohibit marketing activities unless the consumer has provided specific authorization. Under HIPAA, marketing activities are prohibited without authorization; however, certain activities are carved out of the definition of "marketing". Those activities include communications by a covered entity to describe health-related products or services provided by or included in a health plan, replacements or enhancements to a health plan, and health-related services available to enrollees that add value to but are not part of the plan. These communications allow plans to advise their enrollees of available additional services or enhancements that may be of interest to the enrollee without requesting authorization. This bill would instead require the plan to get specific authorization for these communications.

In addition to HIPAA, health plans in New York are also subject to insurance privacy regulations.[1] These regulations were adopted in accordance with the Gramm-Leach-Biley Act to protect the privacy of insurance consumers. These regulations apply to licensees of the Department of Financial Services, including health maintenance organizations. This regulation not only applies to disclosure of nonpublic personal health information but also to nonpublic personal financial information. The regulation sets forth notice requirements, the ability to opt out of disclosure of nonpublic personal financial information, and the requirement to opt in to disclosure of nonpublic personal health information, with certain exceptions (e.g., claim administration, fraud detection, utilization review) that align with where disclosure is permitted without authorization under HIPAA. Further, state regulations provide standards regarding authorization to release nonpublic health information, including the information that must be contained in it and that it shall be valid for a specific time, but no longer than 24 months.[2]

While this bill contains exemptions related to protected health information and entities covered by HIPAA, the exemptions are limited and do not fully correspond with HIPAA. For example, the exemption for covered entities under HIPAA only applies to the extent that the covered entity maintains patient information in the same manner as protected health information under HIPAA. To fall under the exemption, health plans would be required to treat all patient information as protected health information, even when HIPAA would not. That exemption is only applicable to covered entities and does not apply to business associates. Additionally, the bill fails to exempt protected health information that is created or maintained by a covered entity or its business associate in accordance with HIPAA. As is currently drafted, the bill exempts out PHI that is collected by a covered entity or business associate governed by HIPAA.

While the overall goals of this bill are laudable – to protect health information that is not otherwise covered by HIPAA – without a clearer exemption for health plan activities, this bill would create overlapping and inconsistent privacy requirements and place additional administrative burdens on

[1] 11 NYCRR Part 420 (Regulation 169).
[2] 11 NYCRR § 420.18.

health plans. As health plans are already covered by extensive state and federal privacy requirements, any additional state privacy laws that do not specifically exempt health plans would complicate health plans' ability to provide health insurance coverage to New Yorkers, create administrative burdens, limit a health plan's ability to work with vendors to provide innovative products or programs for their members, and increase costs which would be felt by New York employers and consumers through higher health insurance premiums.

For all the foregoing reasons, the New York Conference of Blue Cross and Blue Shield Plans opposes the enactment of this bill.

Respectfully submitted,

HINMAN STRAUB ADVISORS, LLC.
Legislative Counsel for the Blue Cross and Blue Shield Plans of New York