1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

February 7, 2025

Via Electronic Mail

The Honorable Kathy Hochul
Governor of New York State
NYS State Capitol Building
Albany, NY 12224

Dear Governor Hochul:

The Future of Privacy Forum (FPF) writes to you regarding S929, the New York Health Information Privacy Act, and its potential to create additional, and potentially unintended, privacy risks for individuals seeking to use health and wellness services in New York. FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.[1]

The New York Health Information Privacy Act (the "Act") intends to create additional safeguards and protections for consumer health data not regulated by the federal Health Insurance Portability and Accountability Act. Health data is uniquely sensitive and should be subject to robust protections.[2] However as currently written the Act diverges from established frameworks for the protection of consumer health data and may exacerbate privacy risks, inadvertently encourage greater data collection, and restrict low-risk data processing that can benefit individuals. As your office considers this bill and any potential for chapter amendments, we urge close attention to the following issues:

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.

[2] Jordan Wrigley, *Out, Not Outed: Privacy for Sexual Health, Orientations, and Gender Identities*, Future of Privacy Forum (Oct. 11, 2024), https://fpf.org/blog/out-not-outed-privacy-for-sexual-health-orientations-and-gender-identities; Deven McGraw & Kenneth D. Mandl, *Privacy Protections to Encourage Use of Health-relevant Digital Data in a Learning Health System*, npj Digital Medicine (2021), https://www.nature.com/articles/s41746-020-00362-8.

(1) Individual rights established under the Act do not have privacy-protective safeguards comparable to other state privacy laws to prevent misuse by bad actors to exfiltrate sensitive data or block access to services;

(2) By extending to individuals who physically enter New York, the Act may encourage additional collection of sensitive geolocation data; and

(3) The lawful purposes for which data is able to be processed under the Act are narrower than comparable state privacy laws and may impede socially beneficial activities.

In order to provide greater context for how the Act aligns and diverges from leading U.S. state frameworks for the protection of consumer health data, we have attached as an addendum a chart comparing the Act to Washington State's My Health My Data Act (2023) and Connecticut's comprehensive consumer health privacy law, which was amended in 2023 to provide heightened protections for consumer health data.

1. **Individual rights established under the Act do not have privacy-protective safeguards comparable to other state privacy laws to prevent misuse by bad actors to exfiltrate sensitive data or block access to services.**

The Act does not clearly permit organizations to authenticate individual rights requests, nor does it explicitly allow organizations to deny a request if they have a good faith belief that the request is fraudulent. The Act grants covered individuals the right to access their regulated health information, the right to immediately revoke authorization for processing regulated health information, and the right to delete their regulated health information.[3] These individual rights generally align with individual rights given to individuals regarding their health data in jurisdictions such as Washington State and Connecticut.[4] However, New York diverges from Washington and Connecticut by failing to establish a framework for the authentication of requests by consumers and their agents.

Washington's and Connecticut's laws both allow for an organization not to honor individual rights requests if it is not able to, "using commercially reasonable efforts," authenticate the request. There is no requirement that requests *must* be authenticated, but as Connecticut makes clear, companies may deny an opt-out request if they have "a good faith, reasonable and documented belief that such request is fraudulent."[5] In contrast, the New York Health Information Privacy Act mandates that organizations "shall make available a copy of all regulated health information about the individual" that the organization maintains, within thirty days of receiving the request. The Act likewise requires compliance with deletion

[3] S929, §§ 1122(2)(c) & 1123(1)-(2).
[4] Wash. Rev. Code § 19.373.040; Conn. Gen. Stat. § 42-518 (2024).
[5] Conn. Gen. Stat. § 42-518(c)(4) (2024).

requests within 30 days of receiving a request. It does not provide any explicit leeway for regulated entities to deny rights requests when the entity is unable to verify the identity of the requestor.[6]

Failing to explicitly allow regulated entities to deny access and deletion requests when they are unable to reasonably verify or authenticate the identity of the requestor could have serious negative implications for individuals' privacy. Given the sensitive nature of the data regulated under the Act, there is potential for bad actors to gain access to an individual's regulated health information. Alternatively, there is also the potential for bad actors to maliciously exercise deletion rights and restrict an individual's access to health services. Creating individual rights without this important safeguard in place may be contrary to the goals of the Act, and has the potential to put the healthcare and health data of individuals at risk. This is especially important because the Act provides that agents - who may have no prior engagement with a business - may exercise these rights on behalf of third parties.

Another notable difference between the Act's obligations and those in Washington and Connecticut concerns the timing of responding to requests. The Act allows regulated entities only 30 days to comply with access and deletion requests, with no opportunity to extend that deadline if necessary. Washington and Connecticut, in contrast, require compliance "without undue delay" and within 45 days at most, provided that regulated entities or controllers may extend the period by an additional 45 days "when reasonably necessary."[7] This timeframe for complying with requests is shorter than either Washington or Connecticut and does not appear to allow for any flexibility in investigating the authenticity of an individual rights request. The Act's shortened compliance timeline for responding to rights requests and potential for liability could create incentives for organizations to comply with potentially fraudulent consumer requests.

2. **By extending to individuals who physically enter New York, the Act may encourage additional collection of sensitive geolocation data.**

The Act applies broadly to include any organization that processes covered health information of an individual physically present in New York, which may incentivize organizations to collect more geolocation data in order to meet compliance obligations. The Act defines regulated entities to include organizations that: (a) control the processing of regulated health information of New York residents; (b) control the processing of regulated health information of any individual *physically*

[6] It could be argued that using commercially reasonable methods to verify or authenticate the identity of individuals submitting rights requests is required for a rights mechanism to be "effective" as required under the Act or to comply with the Act's data security obligations. The risk of overcompliance, however, makes it unlikely that regulated entities would read such requirements into the law and risk being subject to an enforcement action.

[7] Wash. Rev. Code. § 19.373.040(1)(g); Conn. Gen. Stat. § 42-518(c)(1) (2024).

present in New York while that person is in New York; or (c) is located in New York and controls the processing of regulated health information.[8] The Act's various protections therefore attach to many individuals who are not New York residents but are physically present in the state regardless of whether the covered entity does business in New York or collected data in New York. The obligations under the Act appear to kick in (and apply retroactively to data collected) the second an individual steps foot in New York, even if for a short layover at LaGuardia airport. This scope is considerably broader than comparable consumer privacy laws which are typically directed toward protecting the data of residents of a particular state.[9]

This broad extra-territorial scope may ultimately negatively impact individuals' privacy. Subjecting organizations that may not have a business presence in New York to the Act if the organization merely processes the regulated health information of anyone physically present in New York while that person is in New York creates operational challenges for organizations across the country. Crucially, the Act makes no mention of whether an entity *knowingly* processes the health data of any individual physically present in New York. Therefore, organizations may find themselves compelled to collect sensitive location data just to determine whether individuals are in New York at any given time - contrary to the Act's goal of reducing the amount of sensitive data collected about individuals.

3. **The lawful purposes for which data is able to be processed under the Act are narrower than comparable state privacy laws and may impede socially beneficial activities.**

The "Lawfulness of processing regulated health information" provisions could be better aligned with existing state comprehensive privacy laws to provide more flexibility for internal business operations consistent with consumers' reasonable expectations. Potentially the most impactful aspect of the Act is its prohibition on processing regulated health information unless doing so is "strictly necessary" for one of seven enumerated permissible purposes or the regulated entity obtains valid authorization for such processing.[10] This requirement is reflective of a broader trend in consumer privacy legislation whereby lawmakers are exploring "substantive data minimization" provisions that narrow the lawful purposes for

[8] S929, § 1120(4) (emphasis added).
[9] The extraterritorial scope of the New York Health Information Privacy Act also raises questions about the dormant commerce clause, given that as written, *any* business in New York must apply these protections to their customers regardless of where in the country the customer is located and any business outside of New York must apply these protections to any customers who enter New York. *See* U.S. Constitution Annotated - Dormant Commerce Power: Overview, Cornell Law school Legal Information Institute (accessed Feb. 2, 2025), https://www.law.cornell.edu/constitution-conan/article-1/section-8/clause-3/dormant-commerce-power-overview.
[10] S929, § 1122(1)(b)(ii).

which entities can collect, use, or disclose personal data.[11] These new substantive data minimization requirements are intended to curtail excessive data collection and use that is unrelated to providing a requested product or service. However, if written too strictly, a substantive data minimization requirement can operate as a *de facto* prohibition on low-risk, socially beneficial activities that align with consumers' reasonable expectations, such as product research and development.

Under the Act, regulated entities would need to obtain valid authorization for numerous low-risk data collection and processing activities, which is a significantly high bar. In contrast, Washington's My Health My Data Act requires opt-in consent for such processing activities and reserves heightened "valid authorization" for higher-risk sales of covered health data.[12] The Washington consent standard, which aligns with the majority of U.S. state comprehensive privacy laws and the E.U.'s General Data Protection Regulation, is robust and meaningful while being more flexible and easier to operationalize than valid authorization. Another approach taken is Connecticut's comprehensive privacy law, which explicitly preserves a consumer health data controller's ability to collect, use, and retain data for certain internal uses:

> The obligations imposed on . . . consumer health data controllers under sections 42-515 to 42-526, inclusive, shall not restrict a . . . consumer health data controller's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or consumer health data controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.[13]

The Act, in contrast, explicitly excludes activities related to research and development from the internal business operations permissible purpose.[14] Allowing research and development consistent with such safeguards will enable consumer health services to engage in socially beneficial research and product development to the benefit of New York residents while still curtailing excessive data collection and sharing with third parties.

---

[11] Jordan Francis, Unpacking the Shift Toward Substantive Data Minimization Rules in Proposed Legislation, IAPP (May 22, 2024), https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-minimization-rules-in-proposed-legislation.

[12] Washington My Health My Data and consumer privacy laws define consent as a "clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement." Wash. Rev. Code §§ 19.373.010(6); Conn. Gen. Stat. §§ 42-515(7) (2024).

[13] Conn. Gen. Stat. § 42-524(b) (2024).

[14] S929, § 1122(1)(b)(ii)(B).

Thank you,
Bailey Sanchez
Deputy Director for U.S. Legislation, Future of Privacy Forum
bsanchez@fpf.org

Jordan Francis
Policy Counsel, Future of Privacy Forum
jfrancis@fpf.org