HEALTH INNOVATION ALLIANCE

August 7, 2023

The Honorable Lina Khan
Commissioner
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580

Submitted electronically to regulations.gov

Dear Commissioner Khan,

The Health Innovation Alliance (HIA) appreciates the opportunity to comment on your proposed rule to modify the Federal Trade Commission's (FTC) Health Breach Notification Rule (HBNR). We are specifically focused on:

- Instituting consistent and reliable privacy policies,
- Ensuring regulations do not impede the development of new treatments and the care of patients, and
- Ensuring any privacy policies do not conflict with HIPAA and other existing privacy laws and regulations.

HIA is a diverse coalition of patient advocates, healthcare providers, consumer organizations, employers, technology companies, and payers who support the commonsense use of data and technology to improve health outcomes and lower costs. We are actively engaged in the policy discussion on ensuring the privacy and security of health information, particularly as health information becomes more liquid. We urge you to ensure any final rule issued by your Commission does not create duplicative regulation for entities engaged in healthcare delivery and that existing healthcare laws and regulations that ensure health information flows to those who need it are not impacted by your rulemaking.

We are concerned that your proposed rule is an overreach of the Commission's authority. Congress is working to improve privacy protections, but it has not yet advanced legislation into law. Some of the proposals Congress is considering would give the FTC authority to take many of the actions it proposes in this rulemaking. However, those authorities have not yet been granted. Instead, the FTC changed its interpretation of the HBNR to expand the reach of the rule in the September 2021 Policy Statement. That FTC action and this proposed rule are both partisan expansions of the Commission's authority and planned activities. Privacy – particularly in healthcare – is not a partisan exercise. We advise that you balance the need to protect health information with the need to ensure protections are consistent and reliable. Your current proposed rule relies on authority the Commission has granted itself. We fear that well-intended proposals to protect consumer and patient privacy in your rule will be challenged and overturned by litigation. This could lead to further confusion and inconsistency in privacy policies.

HIA recognizes that increasing health information liquidity requires privacy and security. In 2020, we released principles to guide Congress in a new health data and privacy framework.[1] We have also worked directly with Congress on legislation to determine whether existing healthcare privacy laws and regulations need to be updated, and if so, how. The Health Data Use and Privacy Commission Act would establish a federal commission to make official recommendations to Congress.[2] More recently HIA worked with Congress to ensure that legislation intended to increase the privacy of consumer data does not unintentionally stop the use of health data in areas like care delivery, licensing, and medical research.[3]

The National Conference of Insurance Legislators (NCOIL) just adopted a resolution HIA drafted to ensure that consumer privacy laws include exemptions for health privacy laws that regulate medical research, patient care delivery, and other aspects of healthcare that are already well regulated. We have attached this model resolution for you to examine to prevent your regulations from inhibiting the active use of health information to produce new treatments and cures, protect patients from harm, and ensure caregivers have accurate information to treat their patients. We ask the Commission to make all changes necessary to guarantee the advances made in healthcare interoperability, medical research, and care delivery are not impeded by this regulation or any other regulations considered by the Commission.

We also urge you to consider adopting model security practices to protect users on the front end. In particular, identity verification for systems or applications using health information can prevent unintended breaches or disclosures. The financial industry is very good at protecting confidential information, and there is no reason healthcare cannot adopt similar technologies. Several practices have proven successful at mitigating unauthorized access to secure systems like including identity attributes in identity proofing, embracing multi-layered solutions, applying intelligent and regular risk assessments, and using technology-based solutions to distinguish legitimate users from malicious bots.

We believe that the estimation that your proposed rule will impact 170,000 entities is an underestimation and misunderstanding of how sweeping your definitions are in this proposal. The definition you propose for a provider includes the phrase "any other entity furnishing health care services or supplies."[4] We fear that this definition is so broad, it may include even simple vendors like corner markets selling the most basic healthcare supplies.

Your proposed definition of breach brings in the well-understood concept of disclosure. Health data governed by HIPAA is routinely disclosed during the course of patient care for categories of activities related to the treatment, payment, and operations of healthcare that surround patient care. These disclosures are allowable under HIPAA so that care delivery can occur. Your proposal could lead to conflicting rules for healthcare entities on whether the data in question is subject to your "authorization" requirement.[5] Routine disclosures of data should be allowed in certain contexts without additional need for authorizations. HIPAA already has exceptions to the HIPAA Breach Notification rule that include unintentional acquisition, access, or use; inadvertent disclosure to an authorized person; and inability to retain protected health information. The FTC should clarify when disclosures do not trigger the proposed, expanded definition of a breach to ensure that the rule is understood and to avoid unnecessary notices to individuals.

---

[1] *Available at* https://health-innovation.org/2020-3-9-health-innovation-alliance-calls-on-congress-to-adopt-new-health-data-and-privacy-framework/

[2] *Available at* https://www.congress.gov/bill/117th-congress/senate-bill/3620/all-info

[3] *See* https://health-innovation.org/2022-6-14-draft-privacy-bill-misses-the-mark-national-framework-is-needed-to-work-for-patients-not-enrich-trial-lawyers/ and https://health-innovation.org/2023-2-28-privacy-legislation-should-not-impede-advances-in-healthcare/

[4] 88 Fed. Reg. 37819, *at* 37823.

[5] *Id*. at 37824.

Finally, you propose that your expansion of the "PHR related entity" definition "will create incentives for responsible data stewardship and de-identification."[6] However, you do not propose what de-identification standards you support or adopt. Consistency in de-identification standards is instrumental for compliance. When California was first considering the California Consumer Privacy Act, the law set definitions for de-identification that were inconsistent with those in HIPAA. This inconsistency could have resulted in medical research stopping in its tracks while compliance officers determined how, or if they could, comply with both requirements simultaneously. We encourage you to cite the existing de-identification standards in HIPAA that are well understood and work to protect privacy and to ensure that proposals like this one do not conflict with existing laws and regulations. Creating duplicative regulation will result in burdensome and costly compliance and confusion – not just for vendors, but for consumers and patients as well.

We appreciate the opportunity to comment on your proposed rule and look forward to working with you to ensure the privacy and security of health information is consistent, trusted, and reliable for patients and consumers.

Sincerely,

Brett Meeks
Executive Director

ATTACHMENT: NCOIL Resolution in Support of Existing Law Exemptions for New Data Privacy Laws

[6] *Id*. at 37825.

616 Fifth Avenue, Suite 106
Belmar, NJ 07719
732-201-4133
CHIEF EXECUTIVE OFFICER: Thomas B. Considine

National Council of Insurance Legislators (NCOIL)

Resolution in Support of Existing Law Exemptions for New Data Privacy Laws

Sponsored by Rep. Forrest Bennett (OK)

Adopted by the NCOIL Financial Services & Multi-Lines Issues Committee on July 20, 2023, and the NCOIL Executive Committee on July 22, 2023.

WHEREAS, consumer information from millions of Americans is being collected, organized, and utilized to better understand consumer behavior, perform research, develop new products and services, and create "big data"; and

WHEREAS, the use of big data has accelerated innovation and produced positive outcomes in the insurance and health care sectors and in a myriad of other industries; and

WHEREAS, big data is being used to revolutionize health care, especially in the acceleration of drug development to treat rare diseases; and

WHEREAS, increased data collection in connection with clinical trials and the use of data to study the impact of drug utilization on patient health are helping to ensure that health care treatments, including drugs, are safer; and

WHEREAS, the protection of consumer data is an important public policy issue; and

WHEREAS, some industries, including the health care and insurance fields and those performing clinical research, are subject to longstanding, comprehensive, and robust data privacy requirements; and

WHEREAS, state legislatures are increasingly considering and enacting legislation that would establish data privacy regimes for data brokers and others not already subject to such a framework; and

WHEREAS, it is imperative to safeguard the confidentiality of a consumer's health records without sacrificing or undermining advances and innovation in health care; and

WHEREAS, the states that have established data privacy regimes for data brokers and others not already subject to such a framework (e.g. Texas and Virginia) have included narrow exemptions in those laws that recognize the requirements clinical researchers must already comply with and avoid the adoption of duplicative and conflicting data privacy mandates; and

BE IT NOW THEREFORE RESOLVED, that the National Council of Insurance Legislators (NCOIL) supports innovation in health care in an environment that protects a consumer's right to privacy; and

BE IT NOW FURTHER RESOLVED, that NCOIL urges states that are considering legislation that would establish data privacy regimes for data brokers and others to incorporate exemptions for:

- Entities or information already subject to existing legislative data privacy regimes;

- Identifiable private information that is subject to the federal regulations established for the protection of human subjects in research (i.e. 45 C.F.R. Part 46 and 21 C.F.R. Parts 6, 50, and 56);

- Identifiable private information that is collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

- Information that is deidentified in accordance with the requirements for deidentification pursuant to Health Insurance Portability and Accountability Act (HIPAA); and

- Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2; and

BE IT NOW FURTHER RESOLVED, that the exemptions encouraged in this Resolution are not intended and should not be interpreted to be exclusive of other exemptions to comprehensive data privacy regimes that states may consider; and

BE IT FINALLY RESOLVED, that a copy of this Resolution shall be sent to the Members of each State's committee with jurisdiction over data privacy laws.