AMERICAN CLINICAL LABORATORY ASSOCIATION

October 27, 2022

Chairwoman Lina Khan
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Ste. CC-5610 (Annex B)
Washington, DC 20580

RE: Trade Regulation Rule on Commercial Surveillance and Data Security, Advance Notice of Proposed Rulemaking (R111004)

Dear Chairwoman Khan,

Please accept the comments of the American Clinical Laboratory Association (ACLA) on the Advance Notice of Proposed Rulemaking, "Trade Regulation Rule on Commercial Surveillance and Data Security".[1] ACLA is the national trade association representing leading laboratories that deliver essential diagnostic health information to patients and providers. ACLA members are at the forefront of driving diagnostic innovation to meet the country's evolving health care needs and provide vital clinical laboratory tests that identify and help prevent infectious, acute, and chronic disease. ACLA works to advance the next generation of health care delivery through policies that expand access to lifesaving testing and information services. Given our decades of experience with patient privacy and data security, we are pleased to offer our perspective to the Commission on alignment of its goals with existing health information privacy and security standards. As described in more detail below, we have several concerns regarding the proposals in the Advance Notice of Proposed Rulemaking. We thank the Commission for providing the opportunity to comment and considering our feedback.

ACLA's responses to questions in the Advance Notice of Proposed Rulemaking are set forth in detail below. The questions to which we are responding follow the section headings. In sum, ACLA believes:

- The Commission should not engage in broad rulemaking and instead should allow Congress to pass comprehensive legislation that provides the clarity and certainty that stakeholders need.
- HIPAA-covered entities and business associates should not be subject to duplicative and conflicting regulation with respect to protected health information.
- De-identified data should remain outside the scope of consumer data privacy and security rules.

[1] 87 Fed. Reg. 51273 (Aug. 22, 2022).

I. The Federal Trade Commission should allow Congress the opportunity to legislate in this area before it engages in rulemaking.

30. Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security?

ACLA urges the Commission to allow Congress the opportunity to develop and pass legislation addressing data privacy, use, and security practices, rather than pursue rulemaking on these topics without clear direction from Congress.

Congress currently is considering legislation to create a comprehensive consumer privacy framework that would govern how different industries and businesses treat consumer data. The American Data Privacy and Protection Act[2] (ADPPA) would apply to most commercial entities and to information that identifies or is linked or reasonably linkable to an individual. Among other things, it would limit the collection, use, or transfer of covered data to specific enumerated purposes; require commercial entities to make certain disclosures about how they use and retain covered data; give consumers various rights over covered data; and require consumer entities to adopt data security and privacy practices. The provisions would be enforceable by the Federal Trade Commission and by state attorneys general, and the legislation would create a private right of action, as well.

There have been other attempts by past Congresses to pass data privacy and security legislation, yet the ADPPA has moved further and has gained more stakeholder input and support than previous efforts. The House Committee on Energy and Commerce has refined the legislation in response to stakeholder suggestions and input from members of Congress who have proposed their own data privacy and security legislation. Whether the ADPPA passes in this Congress, or whether it or another piece of legislation with the same or similar framework is reintroduced in a future Congress, there appears to be momentum in the country for a comprehensive legislative approach to consumer data privacy and protection. The three Commissioners who voted in favor of proceeding with this rulemaking process and the two Commissioners who opposed it all voiced their preference for Congressional action on these topics and enthusiasm for the serious efforts being made in Congress to pass legislation.[3]

---

[2] H.R. 8152, 117th Congress.

[3] *See* 87 Fed. Reg. 51287, Statement of Commission Chair Lina M. Khan ("The recent steps taken by lawmakers to advance federal privacy legislation are highly encouraging, and our agency stands ready to continue aiding that process through technical assistance or otherwise sharing our staff's expertise."); *id.* at 51288, Statement of Commissioner Rebecca Kelly Slaughter ("I am delighted that Congress appears to be making substantial and unprecedented progress toward a meaningful privacy law, which I am eager to see pass…"); *id.* at 51292, Statement of Commissioner Alvaro M. Bedoya ("The bipartisan [ADPPA] is the strongest privacy bill that has ever been this close to passing. I hope it passes soon…"); *id.* at 51293, Statement of Commissioner Noah Joshua Phillips ("I have said, repeatedly, that Congress—not the Federal Trade Commission—is where national privacy law should be enacted. I am heartened to see Congress considering such a law today and hope this Commission process does nothing to upset that consideration."); *id* at 51298, Statement of Commissioner Christine S. Wilson ("I am heartened that Congress is now considering a bipartisan, bicameral bill that employs a sound, comprehensive, and nuanced approach to consumer privacy and data security. The [ADPPA] rightly has earned broad acclaim in the House

ACLA's member laboratories need clarity and certainty about what laws apply to them, what is expected of them, and the timelines for compliance. The amorphous set of issues and concerns set forth in the Advance Notice of Proposed Rulemaking, without a clearly-defined scope and articulable standards of conduct for businesses and stakeholders, yields the opposite. Rather than moving forward on its own, the Commission should allow Congress to develop and pass comprehensive legislation that has defined parameters and that articulates a defined enforcement role for the Federal Trade Commission. In addition to providing clarity and certainty, the legislative process is better-suited to balance the interests of all affected parties than administrative rulemaking is.

II. Healthcare covered entities, which already employ robust privacy and security measures required under HIPAA, should not be subject to duplicative or conflicting regulations by the Commission.

2. Which measures do companies use to protect consumer data?

3. Which of these measures are prevalent?

ACLA members and other "covered entities" that comply with the Privacy Rule and Security Rule under the Health Insurance Portability and Accountability Act (HIPAA)[4] should not be required to comply with duplicative – or conflicting – data privacy and security regulations issued by the Commission. HIPAA comprises a national, consistent patient privacy and data security framework that impacts nearly every aspect of the business of health care. The type of personally-identifiable health information that is subject to HIPAA protections should not be within the scope of any Commission rulemaking on consumer data protections. This is the general approach included in the ADPPA, under which entities that are in compliance with HIPAA's data privacy requirements are deemed to be in compliance with the related requirements of the ADPPA with respect to data that is subject to such regulations.

HIPAA-covered entities and their business associates[5] comply with the Privacy Rule, which "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and

Committee on Energy & Commerce and the Subcommittee on Consumer Protection and Commerce, and is moving to a floor vote in the House.").

[4] Pub.L. 104-191.

[5] Covered entities include health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA. A business associate is an entity or person who is not a member of a covered entity's workforce and who creates, receives, maintains, or transmits protected health information for consulting, accounting, administration, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities billing, benefit management, practice management, and other purposes. *See* 45 C.F.R. § 160.103.

disclosures that may be made of such information without an individual's authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections."[6] The Privacy Rule's "minimum necessary" standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. In addition, the covered entity's policies and procedures must identify those within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access.

HIPAA-covered entities also comply with the Security Rule, which requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information (e-PHI). Generally, covered entities must identify and protect against reasonably anticipated threats to the security or integrity of e-PHI, protect against reasonably anticipated impermissible uses or disclosures of the information, and ensure compliance by their workforce. Covered entities perform risk analyses as part of their security management processes: they evaluate the likelihood and potential risks to e-PHI, implement appropriate security measures to address those risks, document the security measures they implement and the rationale for their choices, and maintain reasonable security protections. Each covered entity is to designate a security official who is responsible for compliance with the Security Rule.

The HIPAA Privacy and Security Rules provide a robust framework to protect personally-identifiable health information from unauthorized use and disclosure. Businesses, consumers, and regulatory agencies have decades of experience with HIPAA and have worked together to make modifications to its privacy and security structures as technology and consumer expectations have changed. The current regulatory framework is able to evolve to protect health information held and received by covered entities without an additional layer of regulation imposed by the Commission.

III. De-identified data should be outside of the scope of any data privacy and security rule.

10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

ACLA believes that de-identified data should be excluded from the scope of any data privacy and security legislation or regulation. Each day, ACLA members use de-identified data for purposes that are beneficial to patients and society, such as research, quality assurance, and development of novel test methods and healthcare data-driven tools to aid healthcare professionals

[6] The HIPAA Privacy Rule, *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

diagnose diseases and conditions. Use of such data should not be curtailed unnecessarily, when the benefit clearly outweighs the minimal or non-existent risk of harm to an individual.

Policymakers have recognized the value of allowing de-identified data to be used, aggregated, and shared with collaborators when the risk of harm to individuals is low. Under the HIPAA Privacy Rule, "health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information" and therefore is not within HIPAA's scope.[7] De-identification is a familiar concept to HIPAA covered entities that comply with the Privacy Rule's de-identification standard and implementation specifications at 45 C.F.R. § 164.514(b). The California Consumer Privacy Act was amended in recent years to adopt this approach, as well, excepting from its scope data that has been de-identified using either method set forth in HIPAA regulations.[8] Similarly, the ADPPA would exclude from the scope of its provisions "covered data" that has been de-identified.

ACLA favors an approach to data use regulation that does not unnecessarily stymie innovation and collaboration when the potential harm to an individual has been mitigated through de-identification.

IV. It is unreasonable for the Commission to consider limiting healthcare companies' ownership or operation of businesses that engage in any specific commercial surveillance practices.

39. To what extent, if at all, should the Commission limit companies that provide any specifically enumerated services (e.g., finance, healthcare, search, or social media) from owning or operating a business that engages in any specific commercial surveillance practices like personalized or targeted advertising? If so, how?

ACLA does not believe that the Commission should place restrictions on healthcare companies from owning or operating businesses that engages in surveillance practices such as personalized or targeted advertising. Specifically, we are concerned about the impact this would have on health care companies' ability to engage in digital marketing activities, even when communicating with individuals who currently are not patients and with health care providers. The Commission has not explained the problem it would solve by singling out entire industries that provide certain services and prohibiting those types of companies from structuring themselves in certain ways, or that such a practice is unfair or deceptive, and it has not provided any evidence of widespread consumer harm caused by targeted advertising by healthcare companies. Moreover, the Commission has not explained its authority to impose this type of business ownership limit. If the Commission were to engage in rulemaking that addresses targeted advertising, it should articulate reasonable standards that all industries are held to for the same type of conduct, rather

[7] 45 C.F.R. § 164.514(a).

[8] Ca. Civ. Code 1798.146(a)(4)(A)(i)-(ii). "De-identified data" is data which cannot reasonably "identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." Cal. Civ. Code § 1798.140(h).

than single out any particular industries for restrictions on their business structures, and it should not limit ownership or operation of businesses engaged in lawful activities. As you know, the Commission can take this kind of action only after clearly identifying the ownership or operation practice that is unfair or deceptive, how the practice causes harm to consumers, how its action would reduce that harm, and that the benefit of curtailing the practice outweighs the cost of doing so.

V. The Commission should not single out the healthcare industry if it imposes data minimization or purpose limitations.

> *46. [S]hould new rules impose data minimization or purpose limitations only for certain designated practices or services? Should, for example, the Commission impose limits on data use for essential services such as finance, healthcare, or search—that is, should it restrict companies that provide these services from using, retaining, or transferring consumer data for any other service or commercial endeavor? If so, how?*

The Commission should not target the healthcare industry if it imposes data minimization or purpose limitations. We are deeply concerned that such an approach could curtail or prohibit use of aggregated and/or de-identified data for research used in the development of clinical diagnostics, drug therapies, and other life-saving medical interventions. This would do grievous harm, and such an action would fail to balance the supposed harm to an individual against the broader benefits to society. In addition, the Commission has not articulated the benefits of restricting companies that provide healthcare services from using, retaining, or transferring consumer data for any service or commercial endeavor, other than the "specifically enumerated services", even when an individual has provided consent for that use, retention, or transfer.

* * * * *

ACLA stands ready to engage with the Commission and share our experiences and expertise to ensure that the Commission's approach aligns thoughtfully with the way that laboratories and other health care providers use and interact with patient information. Thank you for consideration of ACLA's comments.

Sincerely,

Susan VanMeter, President
American Clinical Laboratory Association