AMERICAN CLINICAL LABORATORY ASSOCIATION

June 25, 2024

The Honorable Cathy McMorris Rodgers
Chair, House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member, House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chair McMorris Rodgers and Ranking Member Pallone:

Thank you for considering the comments of the American Clinical Laboratory Association (ACLA) on the updated discussion draft entitled *American Privacy Rights Act* (APRA). ACLA is the national trade association representing leading laboratories that deliver essential diagnostic health information to patients and providers by advocating for policies that expand access to the highest quality clinical laboratory services, improve patient outcomes, and advance the next generation of personalized care.

ACLA members are committed to protecting the privacy and security of individuals' personal data and agree that compliance with federal and state privacy laws is of the utmost importance. The association shares the Committee's goals of eliminating the existing patchwork of privacy laws and regulations and creating a workable framework for privacy protections that is sensible and balanced. To that end, ACLA provides comments and input on the following provisions of the updated draft:

- Interaction between the Health Insurance Portability and Accountability Act (HIPAA) and APRA
- State law preemption
- Implementation timeline
- Private right of action
- Privacy notice
- Transfer of data
- Definitions

A. Interaction between HIPAA and APRA

In previous versions of the discussion draft, Sec. 118(b)(3)(B)(ii-iii) would have "deemed" an entity that is required to and does comply with the HIPAA privacy and security rules to be in compliance with APRA, which was confusing. It was not clear whether a HIPAA covered entity with a robust privacy and security compliance program that inadvertently makes an unauthorized disclosure of the data of only a few individuals would be considered out of compliance with the HIPAA privacy and security rules and therefore not in compliance with APRA.

ACLA is pleased to see this section updated to state more clearly that a covered entity or service provider that is required to comply with certain specified federal privacy and data security laws and regulations (including but not limited to HIPAA) shall not be subject to APRA, solely and exclusively with respect to any data subject to the requirements of such laws and regulations. ACLA views this amendment as a significant improvement that should exempt from APRA uses and disclosures of data governed by HIPAA privacy requirements, including protected health information and data that has been de-identified under HIPAA.

While the new exemption for data governed by other federal privacy and data security laws is helpful, it is important to note that many clinical laboratories operate as hybrid entities under HIPAA – meaning that they may conduct not only functions that make them HIPAA covered entities, but also certain other functions not governed by HIPAA, which may or may not be regulated separately by other federal laws. To the extent that clinical laboratory companies may not be exempt from the application of APRA completely, its other provisions may have an impact on clinical laboratories, and those impacts should be considered in order to avoid potential unintended consequences.

B. State Law Preemption

The purposes of APRA are to "establish a uniform national data privacy and data security standard in the United States to prevent administrative costs and burdens from being placed on interstate commerce" and to "expressly preempt laws of a State or political subdivision of a State,"[1] yet Sec. 118(a)(3)(A) and (N) would undermine those purposes and have the opposite effect. As drafted, APRA would not be construed to preempt provisions of State laws, rules, regulations, and requirements that "protect the privacy of health information, healthcare information, medical records, HIV status, or HIV testing,"[2] among other State provisions. ACLA members and other health care entities already have to comply with HIPAA and with a patchwork of state laws, and this exception from preemption and the others would leave that patchwork intact.

ACLA urges the Committee to amend APRA Sec. 118(a)(3)(A) and (N) to preempt state laws on the subject matters covered by APRA, including "consumer privacy and consumer health privacy protection laws of general applicability." Further, APRA should amend HIPAA such that HIPAA also preempts state laws on the subject matter covered by HIPAA. This would help effectuate the goal of eliminating the patchwork of state laws.

C. Implementation Timeline

As written, the law would be effective 180 days after enactment. Respectfully, this is an inadequate amount of time for affected entities to understand the scope of the law, for the Federal Trade Commission to issue clarifying regulations and/or guidance, and for affected entities to develop and operationalize compliant privacy policies, consents, trading partners agreements, centralized mechanisms, etc. ACLA urges the Committee to change the effective date such that it is two years after enactment, which would align with centralized consent and opt-out mechanism

[1] APRA Sec. 118(a)(1).
[2] APRA Sec. 118(a)(3)(N).

provision in Sec. 106(b) of the draft legislation.

D. Private Right of Action

ACLA members are deeply concerned that inclusion in APRA of a private right-of-action by individuals would incentivize frivolous and nuisance lawsuits. The Committee should remove Sec. 117 of the draft in its entirety. If the Committee does not remove the private right-of-action, then Sec. 117 should be amended to include measures aimed at disincentivizing meritless lawsuits, such as a "loser pays" provision that clarifies that an unsuccessful plaintiff is responsible for the attorney's fees of the defendant covered entity.

ACLA appreciates the draft has been updated in Sec. 117(b) to include the opportunity to cure in actions for injunctive relief, but this section needs further clarification. Sec. 117(b)(1) says an individual must provide the entity 30 days written notice of the specific provisions being violated prior to filing an action. However, Sec. 117(b)(2) says a cure if possible "if within the 60 days the entity cures the noticed violation and provides the person an express written statement that the violation has been cured…". Since the intended effect of a cure is to obviate the need for an action for injunctive relief, and a cure may reasonably take up to 60 days to be effectuated in some cases, the notice period in Sec. 117(b)(1) should be extended from 30 to 60 days to conform to the 60-day cure period in Sec. 117(b)(2), such that if a cure is rendered within 60 days after the notice, no civil action for injunctive relief would be permitted.

E. Privacy Notice

Section 104(b)(4) of APRA would require a covered entity and a service provider to include in its privacy policy information about "the length of time the covered entity or service provider intends to retain each category of covered data, or if it is not possible to identify that time frame, the criteria used to determine the length of time the covered entity or service provider intends to retain each category of covered data." This approach is at odds with how ACLA members and other regulated entities develop their retention policies. More typically, retention policies are developed based on the type of record (*e.g.*, test orders, claims reimbursement), not categories of data contained in them. A customer number or name may be subject to multiple retention policies with different lengths of time. We recommend striking Sec. 104(b)(4) from the content of a privacy policy.

APRA Sec. 104(e) would require a covered entity that makes material changes to its privacy policy to provide each affected individual with advance notice of the change and a means to opt-out of the processing or transfer of covered data subject to the change. This is bound to be extremely costly and burdensome to APRA covered entities, so notice to "each affected individual" should be allowed via a conspicuous website posting that is accessible to any site visitor for a period of time before the change (*e.g.*, 14 days). ACLA recommends striking Sec. 104(e)(2) on direct notification to remove confusion about which method is required for notification.

Previous versions of the APRA discussion draft required that so called "large data holders" must retain and publish on their websites each previous version of privacy policies for 10 years. ACLA is pleased to see the current draft updated to apply prospectively so entities can prepare for retention of such policies.

F. Transfer of Data

The definition of "transfer" at Sec. 101(58) indicates that sharing or disclosing covered data is encompassed by this definition when it is done "for consideration of any kind or for a commercial purpose". Further clarity on what qualifies as "commercial purpose" is needed since virtually *every* transfer of data of this sort made by a U.S. healthcare entity could be considered "commercial", particularly without any qualification of "valuable consideration." In addition, the definition should be amended to exclude transfers to a service provider. Otherwise, consumers will have the right under Section 106 to opt out of transfers to service providers. Such a right would make it impractical for many businesses to use service providers at all.

Section 102(c)(4) prohibits an APRA covered entity from transferring "sensitive covered data", "biometric information", or "genetic information" to a third party without the express consent of the individual, unless the transfer is for a permitted purpose set forth in paragraphs (2), (3), or (4) of Sec. 102(d). ACLA members and other clinical laboratories oftentimes do not have an opportunity to obtain affirmative express consent from an individual, as they usually do not have face-to-face contact with patients, and they often need to transfer such data to third parties for legitimate reasons other than legal obligations. ACLA is pleased to see an exemption for "compliance with legal obligations imposed by Federal, State, Tribal, or local law" in Sec. 102(d)(2). However, the Committee should amend that the transfer requirements and prohibitions in Sec. 102(c)(4)(A) and (B) to add at the beginning of each, "Unless otherwise permitted under Federal, State, local, or Tribal law." To simplify the exemption in Sec. 102(d), we would recommend striking from the introductory clause of Sec. 102(d), "if the covered entity or service provider can demonstrate that the collection, processing, retention, or transfer is necessary, proportionate, and limited to such purpose", and retaining "Subject to the requirements in subsection (b) and (c), a covered entity may collect, process, retain, or transfer, or direct a service provider to collect, process, retain, or transfer covered data for the following purposes:".

Previous versions of the APRA discussion drafts did not include exemptions for individual opt-out of the transfer of an individual's covered data. This did not align with requirements clinical laboratories must comply with to report certain information to public health authorities for the purpose of controlling infectious disease outbreaks. ACLA is pleased to see this concern addressed by Sec. 106(a)(1)(D) in APRA.

G. Other Definitions

Certain definitions in the APRA not referenced above should also be clarified.

De-identified data (Sec. 101(18)): The definition of "de-identified data" provides that data that is considered de-identified under HIPAA is de-identified under APRA, unless it is provided to an entity that is not a HIPAA covered entity and that entity fails to meet certain requirements. ACLA recommends that APRA should make it clear that a HIPAA covered entity that has complied with HIPAA requirements for de-identification at the time of disclosing such data to a third-party bears no further responsibility under APRA for subsequent actions of the third party; any such responsibility should lie with the third party. An APRA covered entity has no control over a third-party's actions, and it may transfer de-identified information subject to the third party's representations to comply with those requirements – and the third party then may renege on its representations. If the Committee does not amend the definition as we have suggested, they

should specify that the third party is solely responsible for complying with the law after receipt of de-identified data. Additionally, this could hinder medical research when there are partnerships with non-HIPAA covered entities if the de-identification standards set by FTC under this draft differ from HIPAA.

Sensitive covered data (Sec. 101(49)): Sec. 101(419)(A)(ii) currently reads: "Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual." To simplify the definition, the Committees should consider amending it to read: "Health information", as that term already is defined at Sec. 101(33).

* * * * *

Thank you for your consideration of ACLA's comments on the updated draft. Please contact Holly Grosholz, Senior Director Government Affairs, hgrosholz@acla.com, with any questions.

Sincerely,

Susan Van Meter
President
American Clinical Laboratory Association