AMERICAN CLINICAL LABORATORY ASSOCIATION

April 3, 2023

Mr. Kevin Stine, Division Chief
Applied Cybersecurity Division, Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive (Mail Stop 2002)
Gaithersburg, MD 20899-8930
Delivered Via E-mail: genomic_cybersecurity_nccoe@nist.gov

RE: NIST IR 8432: Cybersecurity of Genomic Data

Dear Mr. Stine,

The American Clinical Laboratory Association (ACLA) appreciates the opportunity to provide comments on the on the National Institute of Standards and Technology's (NIST's) March 3, 2023, initial draft internal report (IR), Cybersecurity of Genomic Data (NIST IR 8432).[1] ACLA is the national trade association representing leading clinical laboratories. ACLA members are at the forefront of driving diagnostic innovation to meet the country's evolving healthcare needs and provide vital clinical laboratory tests that help identify and prevent infectious, acute, and chronic disease.

ACLA appreciates NIST's consideration of the unique attributes of genomic data and the specific cybersecurity and privacy issues it presents, and we are supportive of appropriate efforts to improve cybersecurity for protecting genomic data. ACLA encourages NIST to prioritize stakeholder engagement in the development of any proposed standards, solutions, and best practices for protecting genomic data. Further, ACLA strongly urges NIST to ensure that NIST IR 8432 will align with the Health Insurance Portability and Accountability Act of 1996 as revised by the Health Information Technology for Economic and Clinical Health Act and their implementing regulations (collectively, HIPAA).

A. The Importance of Alignment with HIPAA – General Considerations

HIPAA comprises a national, consistent health data privacy and security framework that impacts nearly every aspect of the business of health care in the United States and has been in place for two decades. ACLA members, other clinical laboratories, other health care providers that conduct standard electronic transactions, health plans, and clearinghouses are already HIPAA covered entities subject to the HIPAA Privacy and Security Rules, and their business associates

[1] Pulivarti R, Martin N, Byers F, Wagner J, Maragh S, Wilson K, Wojtyniak M, Kreider B, Frances A, Edwards S, Morris T, Sheldon J, Ross S, Whitlow P (2023) Cybersecurity of Genomic Data. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8432 ipd, *available at* https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8432.ipd.pdf.

are as well. While some breaches of privacy or security have been due to causes beyond the reasonable control of the entity in possession of the data, it is likely that many more have been caused by the entity's failure to adhere to HIPAA standards, rather than the inadequacy of the standards themselves. Therefore, before proposing any new privacy or security standards that would be inconsistent with or significantly different from HIPAA, NIST should identify the specific inadequacy in HIPAA that the new proposal is seeking to address, and any such proposal should be narrowly tailored to address that deficiency to the extent possible under the law. To the extent that NIST proposes solutions or best practices that align with HIPAA and enable better implementation of that existing framework, such proposals are more likely to be supported and widely adopted. Additionally, any proposed solutions or best practices should seek to align NIST's control functions of identify, protect, detect, respond, and recover with HIPAA, to make the recommendations more robust.

HIPAA is not the only privacy and security framework to which ACLA laboratories may be subject. Some ACLA laboratories are also subject to the European Union's General Data Protection Regulation (GDPR), and there are several states that have enacted privacy and security legislation that, like the GDPR, may be more stringent than, or otherwise inconsistent with, HIPAA. ACLA encourages NIST to focus its efforts on enabling practical and effective strategies for appropriate implementation of HIPAA in the United States.

B. De-identification

ACLA is concerned about unintentional barriers to clinical research posed by NIST IR 8432 draft report's suggestions of the need for heightened requirements for de-identification of genomic data.[2] The HIPAA methodologies for de-identifying data[3] are well-established approaches that have been operational for decades and that allow clinical laboratories to share and use de-identified information for research purposes. Although re-identification risk with genomic data under existing de-identification approaches is theoretically possible, it currently cannot be done without extraordinary measures. It is standard for clinical research data use agreements to require the recipient to agree that it will not attempt re-identification.

The incongruence between the draft NIST IR 8432 and existing HIPAA approaches to de-identified data could disrupt clinical research in a significant way. NIST's statement that genomic data would not meet the standard for HIPAA "safe harbor" fails to take into account that genomic data may come in different forms and refer to different scopes of data. Not all use cases would necessarily require use of the types of data that would facilitate the reidentification risk highlighted in the draft report. Using such broad terminology unnecessarily restricts companies from engaging in certain activities and developing products that could help treat patients and diagnose conditions. ACLA urges NIST to recognize that the HIPAA methodologies for de-identifying data[4] are well-established and sufficient approaches that allow clinical laboratories to share and use de-identified information for research purposes.

---

[2] *Id.* at Section 4.3.1, page 17, lines 759-764.
[3] 45 C.F.R. § 164.514(b).
[4] 45 C.F.R. § 164.514(b)).

C. Homomorphic Encryption

Draft NIST IR 8432 contemplates federated homomorphic encryption as one possible approach for de-identification of genomic data.[5] Although we agree with a federated homomorphic encryption demonstration project for analysis of genomic data in precision medicine or oncology,[6] this method of data encryption is currently impractical, cumbersome, and not ready for widespread implementation. While NIST argues that homomorphic encryption would provide a better way to ensure data integrity, ACLA members have found that a simpler file integrity monitor can achieve the same goals without the overwhelming task of homomorphic encryption.

* * *

ACLA appreciates the opportunity to provide these comments and would be pleased to serve as a resource for the National Institute of Standards and Technology for generating and managing genomic data in a way that aligns with HIPAA. If you have any questions, please contact Holly Grosholz at hgrosholz@acla.com or Joan Kegerize at jkegerize@acla.com.

Sincerely,

Susan Van Meter, President
American Clinical Laboratory Association

[5] NIST IR 8432 at Section 5.6.2, page 28, lines 1130-1145.
[6] *Id.* at Section 5.6.2, page 28, lines 1138-1139.