INFORMATICS PROFESSIONALS. LEADING THE WAY.

April 19, 2024

Assistant Attorney General Matthew Olsen
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC
20530

Assistant Attorney General Olsen:

Thank you for the opportunity to submit comments to the noticed for proposed rulemaking (ANPRM) join provisions regarding access to Americans' bulk sensitive personal data and government-related data by countries of concern. As the leading organization of professionals working with healthcare data and protected health information (PHI), the American Medical Informatics Association (AMIA) supports the Administration's efforts to protect American data and encourages the recognition that data privacy policies must also account for preservation of health innovation opportunities and informing public health.

AMIA is the professional home for more than 5,500 informatics professionals, representing frontline clinicians, researchers, public health experts, and educators who bring meaning to data, manage information, and generate new knowledge across the research and healthcare enterprise. As the voice of the nation's biomedical and health informatics professionals, AMIA plays a leading role in advancing health and wellness by moving basic research findings from bench to bedside, and evaluating interventions, innovations and public policy across care settings and patient populations.

AMIA's Public Policy Principles[1] contains several Principles may address the issue in the ANPRM, including:

- Health IT Safety
- Data Sharing in Research
- Health IT Data Standards & Interoperability
- Population & Public Health
- Health Data Privacy

Health IT Safety

As the department further considers rulemaking on this issue, AMIA encourages:

1. Efforts to fund research that contributes to and advances health IT safety, including research that develops new IT to improve safety, as well as evaluates the safety of live health IT systems as used in practice, so that a robust evidence base can inform the total health IT lifecycle and identify ways to remediate risks.

[1] AMIA Public Policy Principles. 2020. Available Here: https://amia.org/public-policy/public-policy-principles

2. Efforts to train and credential health informatics experts at all levels, such as physicians, nurses, pharmacists, and researchers, to identify and address health IT safety issues.
3. Regulatory and oversight frameworks that are designed to be proportional to the risk of the activity, and reflective of clinicians' ability to intervene in the activity being informed by health IT.[2]
4. Policies, strategies, and technical standards that facilitate health IT-related patient safety event reporting by front-line clinicians and patients.[3]
5. Development and refinement of best practices meant to enable healthcare organizations to address health IT safety within and across organizations, such as ECRI's Copy & Paste Toolkit[4] and ONC's SAFER Guides.[5]
6. Contracts and practices that promote safety, disclosure of errors, bugs, design issues, and software-related hazards, while permitting protection of intellectual property.[6]

Data Sharing in Research

AMIA believes that data sharing among stakeholders is critical to advance scientific discovery, improve benefit and risk assessments, conduct comparative effectiveness research, improve patient safety, and promote biomedical research rigor, transparency, and reproducibility. AMIA also asserts that data sharing should preserve and protect patient privacy and autonomy. To safely and effectively realize the advantages of data sharing, AMIA strongly urges the Department and the Administration to invest in sustainable funding for clinical informatics education programs and other underlying infrastructure of data curating, protecting, and sharing.

Additionally, AMIA encourages:

1. The implementation of data standards that can be used for consumer- and patient generated data, electronic health records, and other data that could be useful to informatics researchers to convey summary data in a usable format, individual participant data and metadata for different types of research to help amplify scientific knowledge while minimizing risks to privacy.[7]
2. Dedicated funding from research sponsors for data curation and sharing efforts so there are sufficient incentives to share, collaborate, and advance data sharing capabilities.[8]

---

[2] Bipartisan Policy Center Health Innovation Initiative, "An Oversight Framework for Assuring Patient Safety in Health Information Technology," Feb. 2013. Available: http://bit.ly/297Ardb

[3] Huerta T., Walker C., Murray K., et al "Patient Safety Errors: Leveraging Health Information Technology to Facilitate Patient Reporting." Journal for Healthcare Quality, 2016 Jan-Feb; 38(1): 17-23

[4] ECRI Partnership for Health IT Patient Safety, "Health IT Safe Practices: Toolkit for the Safe Use of Copy and Paste," ECRI Institute, Feb. 2016. Available: http://bit.ly/297z7qo

[5] Sittig, D.; Ash, J.; Singh, H. "ONC Issues Guides for SAFER EHRs" Journal of AHIMA 85, no.4 (April 2014): 50-52

[6] Goodman, K., Berner, E., Dente, M., et al "Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force," Journal of the American Medical Informatics Association, 2011 18: 77-81

[7] National Academy of Medicine (formerly Institute of Medicine) "Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk," Jan. 2015 http://bit.ly/1Vwtnbi

[8] Borne, P., Lorsch, J., Green, E., "Perspective: Sustaining the big-data ecosystem," Nature. November 2015. 527, S16– S17

3. Institutional rewards for those who create and/or contribute to public datasets and software that others find useful so that incentives exist for those who create as well as those who analyze data.[9]
4. The creation of harmonized regulatory and/or policy frameworks for data sharing, including: data use agreements; data sharing plans; human-subjects reviews and federal, state and local privacy requirements to minimize barriers to sharing data.[10]
5. The incorporation of the FAIR data principles (findable, accessible, interoperable and reusable) to optimize the use of resources and data.[11]
6. Efforts to develop evaluation frameworks that assess the value of data sharing and curation.

Health IT Data Standards & Interoperability

AMIA believes that clinical, research, and health information technology (HIT) systems must be able to exchange biomedical, clinical, and health data consistently and reliably while using computable formats that preserve the intended meaning of the data. Access to and reliable use of these electronic data at scale requires that established, consistent, well-published, and openly available HIT standards be used to specify the formats and values for biomedical, clinical, and health data. To ensure the consistency and comparability of biomedical and clinical data, HIT standards must have coordinated development, open participation, and transparent governance. Whenever possible, one canonical specification should be designated as the preferred representation for each biomedical, clinical, and health data standard that are required for defined use-cases related to optimizing health and healthcare. As such, AMIA encourages:

1. The development and management of HIT standards as a public good, operated in a nonprofit, non-proprietary basis, with low barriers to review, reference, or use.
2. Efforts to recognize and address stakeholder motivations, aims, activities, business models, and information needs in the specification of HIT standards so as to increase the value of their adoption by users and improve ease of implementation.
3. Adequate funding for the development, management and maintenance of HIT standards, and the SDOs that create them, due to the enormous positive impact on society HIT interoperability can have.

Population & Public Health

Given the recent experience of the fast-spreading COVID-19 pandemic, AMIA encourages the Department to prioritize the exchange of information to advance public health. This applies nationally, but globally as well. When medical, social, and public health services work together, the community benefits. As such, AMIA encourages the department to consider ways to exchange data internationally while still preserving privacy of sensitive data. AMIA encourages:

1. Better (1) integration, (2) interoperability, and (3) bi-directional sharing of data, information, and knowledge across care delivery, public health agencies, and community-

[9] Piwowar, H., Vision, T., "Data reuse and the open data citation advantage," Peer J. 2013. 1:e175
[10] Taichman, D., Backus, J., Baethge, C., et al. "Sharing Clinical Trial Data: A Proposal From the International Committee of Medical Journal Editors," Annals of Internal Medicine. 2016. doi:10.7326/M15-2928
[11] "FAIR data principles," The Future of Research Communications and e-Scholarship. Available at https://www.force11.org/group/fairgroup/fairprinciples

based organizations to inform policy, drive prevention and disease management efforts, and support community resource information sharing.
2. Work to develop nationally and internationally (e.g. WHO) scalable, multi-jurisdictional approaches to common public health work flows (e.g., electronic case reporting) for broad dissemination.[12]
3. Dedicated funding for training of public health informatics professionals analogous to NIH funding to ensure the continued evolution of the field.[13]
4. Development of more sophisticated approaches for protecting individual's confidentiality while implementing strategies to improve population health outcomes.
5. Investment in public health informatics workforce training to build competencies and capacity at every level where information is generated, managed, and used for population health.[14]

The threat of communicable risk, contaminant risk, and other threats to public health necessitates broad access to health data with severe penalties for misuse.

Health Data Privacy

AMIA recognizes that the volume, variety, and velocity of health data are rapidly growing across care delivery, research, community, and commercial settings within our nation and internationally. AMIA appreciates the Administration's acknowledgement that health data must be protected to reduce risk of harm to individuals. An individual's privacy protections must be consistently maintained, and their privacy preferences respected across clinical, research, community services, and commercial use of their health data. Health data must always be collected, managed, and shared in ways that minimize the risk of reidentification of individuals. One solution to address the risk of privacy breaches to individuals who may be part of a bulk data set is to improve the public's health data literacy. This ensures that the individuals providing PHI understand that their information is data, becomes part of a much larger data set, the associated risks, and how they can mitigate or identify breaches.

AMIA supports the Department's considerations of:

1. Federal privacy policy that lays a foundation for (1) individual data rights and protections; (2) obligations and custodial duties for data owners, managers, and users; and (3) data use prohibitions across jurisdictional and geographic boundaries, while also establishing a process for jurisdictions to address local needs and norms.
2. Federal protections from harassment, targeting, unwanted marketing, bias, discrimination, stigma, and exploitation resulting from use, disclosure, or reidentification of health data.
3. Transparency in how an individual's health data are used or disclosed once collected or generated through clear, easily accessible, and readable explanation of permitted uses, including when being shared internationally.

---

[12] Digital Bridge Project. Available at: http://www.digitalbridge.us/

[13] SHINE Fellows. Available at: http://www.shinefellows.org/

[14] LaVenture M, Baker B. Developing an Informatics-Savvy Health Department: From Discrete Projects to a Coordinating Program Part II: Creating a Skilled Workforce. J Public Health Manag Pract. 2017 Nov/Dec;23(6):638-640.

4. Permissions or consents for data use and disclosure that are accurate, granular, timely, presented in formats that support accessibility by all, understandable across target education levels, revocable, and that are collected from individuals without duress or misleading statements.
5. Development of data standards that can represent and enact privacy policy, such as through tagging (e.g. Security Labels)[15] and metadata (e.g. provenance).[16] Publicly funded research programs that promote responsible data sharing and that seek to be broadly inclusive of diverse and under-represented populations.
6. Explicit accommodation for data access, aggregation, and sharing for purposes of public health.
7. Computable audit trails and accounting of disclosures so individuals can determine who accessed their data, when, and for which purposes.
8. Security systems and controls that protect data in transit and at rest.
9. Authentication of individuals and entities and verification of authorization to receive health data before data are shared.
10. Adequate funding for investigation and enforcement of privacy laws, with consequential penalties for individuals and businesses that violate laws and regulations, and with individual redress for harm.
11. Policies that provide individuals the opportunity to securely dispose of or transmit or download their health data in the event of a transfer of ownership or in the case of a company ending or selling its business.
12. Policies that confer health data protections to non-health data, when non-health data are applied to represent an individual's health and wellness, or when such data are used for purposes of health care delivery, medical research, or public health.
13. Ongoing funding for research to develop tools and strategies necessary to minimize the risk of reidentification, increase data privacy and security, and promote data literacy.

AMIA recognizes this difficulty of advancing the health of individual's and groups by aggregating and learning from data while also trying to protect PHI privacy for Americans. AMIA appreciates the Administration's attention to this issue and looks forward to continuing to serve as a resource to address data security without stifling innovation and population health.

***

If you have questions or require additional information, please contact AMIA's Vice President of Public Policy, Reva Singh, at rsingh@amia.org.

Sincerely,

Reva Singh

Reva Singh, JD, MA

[15] A security label is a concept attached to a resource or bundle that provides specific security metadata about the information it is fixed to. See more at: https://www.hl7.org/fhir/security-labels.html

[16] Provenance of data is a record that describes entities and processes involved in producing and delivering or otherwise influencing that data. Provenance provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility. Provenance assertions are a form of contextual metadata and can themselves become important records with their own provenance. See more at: https://www.hl7.org/fhir/provenance.html

Vice President of Public Policy