November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230
Submitted electronically via http://www.regulations.gov

RE: Request for Comment - Developing the Administration's Approach to Consumer Privacy

The American Medical Informatics Association (AMIA) is pleased to provide input that will inform the administration's approach to consumer privacy.

Health informatics is the 60-year field of study concerned with data collection, analysis, and application, within broad domains of health, including healthcare delivery, public health, consumer health, clinical research, and translational research. AMIA is the professional home for more than 5,500 informatics professionals, representing front-line clinicians, researchers, educators and public health experts who bring meaning to data, manage information, and generate new knowledge across the health and health care enterprise.

AMIA applauds the administration for initiating an overdue conversation on how to best protect consumer data privacy. The principles described, and concepts supported by the initial proposal are the right ones to be included in this conversation. This RFC will serve as a useful foundation for more in-depth conversations.

In representing the nation's biomedical and health informatics professionals, our views are necessarily tethered to our experience with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Protections for Human Subjects Research, also known as the Common Rule. These health and research "sector" specific rules dictating the data rights and responsibilities of patients, clinicians, participants, and researchers should serve as important and informative inputs to this conversation on consumer data privacy. This is not to suggest that either HIPAA or the Common Rule should apply to the consumer data ecosystem. Rather, as the line between consumer and medical information systems and devices continues to blur, the administration must strive to craft concordant privacy policies across both health and consumer data ecosystems.

First, we note that several facets of HIPAA and the Common Rule are reflected in the RFC's Privacy Outcomes and High-Level Goals (see Appendix A for a crosswalk). **AMIA recommends that the administration examine both HIPAA and the Common Rule closely and develop an explicit High-Level Goal to harmonize "consumer sector" data privacy policies with other sectors, especially the "health sector."** We note that the feared "patchwork" of different state policies, is the reality for healthcare data. This issue has become more pronounced in the era of

digital health records, creating challenges to information exchange, complicating compliance, and generating perverse outcomes based on variable interpretation.

A simple example involves adjoining states – New Jersey and Pennsylvania – with differing policies on HIV/AIDS data. Clinicians in New Jersey who treat a patient from Philadelphia would not be able to access this kind of information when the patient arrives at a hospital in their state, despite the high importance of such data to factor into treatment decisions. Pennsylvania has more restrictions on which data can be available for purposes covered by HIPAA. This same patient, when requesting their data from the New Jersey hospital to take back with them to Philadelphia is unlikely to receive their data, according to a review of common records request practices.[1]

This simple and all too common example highlights the difficulty introduced by discordant data privacy policies. One the one hand, the patient's preference to keep HIV/AIDS data partitioned from his other clinicians may be achieved, but at a potentially dangerous cost to her and her clinicians. Meanwhile, the example also highlights how HIPAA is implemented through a mix of prescription and interpretation. The interpretation – and differences thereof – have led to wild variations in application and perversely inhibited patients from their right to access their data, despite more than two decades' experience with this right.[2]

To avoid similar challenges with future privacy rules, **AMIA encourages the administration to ensure that federal rules lay a common foundation across jurisdictional and geographic boundaries while also providing a process for jurisdictions to address local needs and norms.** Revision of HIPAA to resolve current challenges might serve as a model for broader privacy rules. As the administration considers both health and consumer sector data policies, it must balance the need for both prescriptive process-oriented policies and outcome-oriented policies. An over-emphasis on vague or difficult-to-measure outcomes without guidance on process will result in the failings of HIPAA – wide variation in interpretation and inconsistent implementation.

Second, we are pleased that the RFC recognizes the place of the consumer in its articulation of user-centric core privacy outcomes for organizations that handle consumer data. As we have stated on numerous occasions and in various forums, AMIA believes that patients should always have access to and control over their health data. [3,4,5] This operating principle should not only apply to the health sector, but across all sectors of the US economy. We strongly encourage the administration to view consumer control of their data as the baseline for its policies. **Rather than being an outcome of organizational privacy practices – as currently described in the RFC – AMIA recommends that consumer access to and control of his or her data be a prerequisite condition and central organizing principle from which other outcomes derive.** This subtle difference will help ensure that the difficulties faced by consumers currently in accessing their data does not continue. Further, this is a measurable, discrete outcome for which others can be built and would not likely need prescriptive processes developed by the government to deliver.

---

[1] Lye CT, Forman HP, Gao R, et al. Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records. JAMA Netw Open. 2018;1(6):e183014. doi:10.1001/jamanetworkopen.2018.3014

[2] Ibid.

[3] https://www.amia.org/sites/default/files/AMIA-2018-2019-Health-Informatics-Policy-Priorities-final.pdf

[4] https://www.amia.org/news-and-publications/press-release/amia-ceo-says-access-%E2%80%98complete-medical-record%E2%80%99-key-patients

[5] https://www.amia.org/news-and-publications/press-release/amia-supports-cms-efforts-reduce-documentation-burden-streamline

November 9, 2018

Finally, AMIA broadly supports the RFC's High-Level Goals for Federal Action, with some caveats. While we agree that "there is a need to avoid duplicative and contradictory privacy-related obligations placed on organizations," it is perhaps equally important to recognize where there are gaps in the regulatory landscape regarding data privacy. Again, this is especially true as consumer and health applications and technologies continue to merge. **AMIA recommends the administration should thus include "closing regulatory gaps" that endanger data privacy to its list of high-level goals.**

AMIA stands ready to help ensure the administration's efforts have the requisite expertise to accomplish the worthy goal of enhancing both consumer privacy and innovation. Should you have any questions or require additional information, please contact AMIA Vice President for Public Policy Jeffery Smith at jsmith@amia.org or (301) 657-1291 ext. 113. We look forward to continued dialogue.

Sincerely,

Douglas B. Fridsma, MD, PhD, FACP, FACMI
President and CEO
AMIA

(Enclosed: *Detailed AMIA Comments regarding the Administration's Approach to Consumer Privacy* and *Appendix A: A comparison of HIPAA and Common Rule provisions to inform the Administration's Approach to Consumer Privacy*)

November 9, 2018

Privacy Outcomes

We are intrigued by the administration's desire to "refocus on the outcomes of organizational practices, rather than on dictating what those practices should be." As we understand it, the vision statement for the administration's approach to consumer data privacy is:

> "…a reasonably informed user, empowered to meaningfully express privacy preferences, as well as products and services that are inherently designed with appropriate privacy protections, particularly in business contexts in which relying on user intervention may be insufficient to manage privacy risks. Using a risk-based approach, the collection, use, storage, and sharing of personal data should be reasonable and appropriate to the context. Similarly, user transparency, control, and access should be reasonable and appropriate relative to context… The Administration is proposing that these outcomes be operationalized through a risk-management approach, one that affords organizations flexibility and innovation in how to achieve these outcomes."

We note a reliance on the operative word "reasonable" and we caution that this construct will need further definition. What is considered reasonable will vary across consumers and organizations, and likely will shift over time. Outcomes 4, 5, and 6 are particularly challenging, given this ambiguity. We also note that fulfillment of this vision will be difficult to assess. In examining these Outcomes, it appears the section is largely written to define users' responsibilities rather than what organizations should do. This emphasis is misapplied: consumers are not responsible for having certain characteristics and organizations should be responsible for performing specific tasks.

AMIA appreciates the RFC's focus on outcomes of organizational practices. However, we encourage the administration to better define "users" as either "consumers," "data holders," or "data processers," depending on the context. Additionally, subsequent versions of these comments should be more specific in describing organizational responsibilities.

Within the health care arena, AMIA believes that informatics is a key to enabling delivery of patient-centered care. Numerous studies have shown that enabling patients to access and transmit all data contained in their electronic health record improves the availability of data for care delivery[6,7] and biomedical discovery,[8] and supports the patient's own health and wellness. Furthermore, encouraging patients to review and contribute directly to their record has been shown to improve their understanding of their own health information,[9] lead to improved self-care,[10] increase the

[6] Klein D., Fix ., et al. (2015). Use of the Blue Button Online Tool for Sharing Health Information: Qualitative Interviews With Patients and Providers. Journal of Medical Internet Research. 2015 Aug; 17(8): e199.
[7] Mohsen, M., Aziz, H. (2015). The Blue Button Project: Engaging Patients in Healthcare by a Click of a Button Perspectives in Health Information Management. 2015 Spring; 12(Spring); 1d.
[8] Chisholm, R., Denny J., et al. (2015) Opportunities and Challenges Related to the use of Electronic Health Records Data for Research. National Institutes of Health Precision Medicine Workshop (Invited White Paper). 2015 Feb.
[9] Esch T., Mejilla R., et al. (2016). Engaging patients through open notes: an evaluation using mixed methods. BMJ Open 2016;6:e010034
[10] Wright E., Darer J., et al. (2015). Sharing Physician Notes Through an Electronic Portal is Associated With Improved Medication Adherence: Quasi-Experimental Study. Journal of Medical Internet Research, 17(10)e:226

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

likelihood of the patient's story being communicated accurately,[11] and improve trust within the doctor-patient relationship.[12]

The administration has already shown its commitment to helping patients gain access to health information through the MyHealthEData initiative.[13] We note, however, that access to and privacy of health information is statutorily guaranteed through HIPAA.[14] It is unclear whether individuals have any rights to access data about themselves in situations in which HIPAA does not apply. While there is still much work to do with getting health data into the hands of patients, as the administration recognizes, we believe that how it encourages the access to these data should be replicated across the federal government.

Making consumer data more widely accessible to consumers will likely have similar supplemental uses that will spur innovation and generate a host of unknown downstream benefits.

High-Level Goals for Federal Action

AMIA broadly supports the RFC's High-Level Goals for Federal Action, with some caveats. While we agree that "there is a need to avoid duplicative and contradictory privacy-related obligations placed on organizations," it is equally important to recognize where there are gaps in the regulatory landscape regarding data privacy. As detailed in a 2016 report from the Office of the National Coordinator for Health Information Technology (ONC), there exist health-related technologies outside the scope of HIPAA known as "non-covered entities" (NCEs).[15] The report further explains that while some NCEs may be regulated by FTC and/or state law, there are others that deal with consumer data that may be not fall under regulation all. Even in cases where FTC does provide consumer protection oversight, it does not provide the same type or level as HIPAA.

The RFC says that "FTC is the appropriate federal agency to enforce consumer privacy with certain exceptions made for sectoral laws outside the FTC's jurisdiction, such as HIPAA." As ONC has noted, however, consumer privacy can still be compromised due to regulatory gaps around access, security, and privacy. The administration should thus include "closing regulatory gaps" that endanger data privacy to its list of high-level goals.

Again, we reiterate the need for stronger language that clearly establishes consumer centricity as a prerequisite condition. We note page 48602 articulates a focus "…on creating user-centric outcomes," but that it is unclear whether consumers or the organizations holding consumer data are users. We also note on page 48603, there should be a distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations. Those who process data are, by definition, controlling it, and the regulations that affect organizations should apply to the processors. We are concerned there may be room to

[11] Varpio, L., Rashotte, J., et al. (2015). The EHR and building the patient's story: A qualitative investigation of how EHR use obstructs a vital clinical activity. International Journal of Medical Informatics, 84(12), 1019-1028
[12] Bell S., Mejilla R., Anselmo M., et al. When doctors share visit notes with patients: a study of patient and doctor perceptions of documentation errors, safety opportunities, and the patient-doctor relationship. BMJ Qual Saf 2016
[13] https://www.cms.gov/newsroom/press-releases/trump-administration-announces-myhealthedata-initiative-put-patients-center-us-healthcare-system
[14] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
[15] https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

sidestep compliance with explicit clarity in this area and we encourage the administration to address the closing of this loophole.

In addition, it should be possible for individuals to require that digital products send their data directly to them, bypassing the company's data storage altogether. This high level goal is related to data ownership, but requires a separate and explicit mention because it is not directly implied that a person buying a FitBit should be allowed to have all of the collected data go no further than their own smartphone. Acknowledging that secondary use of this data may be part of the company's business model, companies would be able to charge different prices for the different options, but under the law the company should be required to offer an option for the patient to prohibit the sending of their data to the company in the first place.

Next Steps and Measures

AMIA applauds the interagency process that went into developing this RFC. In this same vein, AMIA recommends the administration look to create a new public-private collaborative that would develop an infrastructure and governance framework that (1) recognizes the diverse and proliferating data from home to community sources and that (2) provides mechanisms for data source identification, registration, and production of relevant metadata for the appropriate re-use of such data.

Finally, the administration should consider developing an ethical framework around the collection, use, storage, and disclosure of the personal information consumers may provide to organizations. AMIA recommends convening an interagency working group that would explore how to enhance the flow of data from traditional and non-traditional sources of consumer systems and devices in a socially and ethically responsible way. This work should then inform coordinated regulatory and enforcement activities. The FTC in coordination with other similar agencies, such as the HHS Office of Civil Rights, should implement the framework that supports trust, safety, efficacy, and transparency across the proliferation of commercial and nonproprietary information resources.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

Appendix A: Comparison of HIPAA and Common Rule provisions with RFC Concepts

Below we highlight a non-exhaustive list of provisions across HIPAA and the Common Rule, which have similarities to concepts expressed in the RFC. A core tension that must be explored is the balance of consumer rights and the need for harmony across jurisdictional and sectoral boundaries.

It is important to acknowledge that these provisions have protected millions of Americans' clinical and research data for more than 20 years. And also, that these policy frameworks have established processes and procedures to address bad actors. The comparative advantage facing the Common Rule is that it does not compete with a bevy of state-level policies. Researchers do not face state-level requirements that go "beyond" the Common Rule, in the way that so many state policies are more restrictive than HIPAA.

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
Transparency: Users should be able to easily understand how an organization collects, stores, uses, and shares their personal information.	Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact	Informed consent must begin with "a concise and focused presentation of the key information that is most likely to assist a prospective subject, or legally authorized representative, in understanding the reasons why one might or might not want to participate in the research. Institutions should update template informed consent forms to meet this requirement. The consent "must be organized and presented in a way that facilitates comprehension." Broad consent for the storage, maintenance, and secondary research use of identifiable private information or

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
	for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans.	identifiable biospecimens (collected for either research studies other than the proposed research or nonresearch purposes) is permitted as an alternative to the informed consent requirements
Control: Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations. However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information.	A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.	
Reasonable Minimization: Data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm.	A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the	

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
	minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.	
Security: Organizations that collect, store, use, or share personal information should employ security safeguards to secure these data. Users should be able to expect that their data are protected from loss and unauthorized access, destruction, use, modification, and disclosure.	A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes.	The final rule includes a new provision that requires the Secretary of HHS to issue guidance to assist IRBs in assuring appropriate privacy and security safeguards. Per the preamble, the guidance might address: the extent to which identifiable private information is or has been deidentified and the risk that it can be re-identified; the use of the information; the extent to which it will be shared, transferred to a third party or otherwise disclosed; the likely retention period; the security controls that are in place to protect confidentiality; and, the potential risk of harm should the information be lost, stolen, compromised or "otherwise used in a way contrary to the contours of the research under the exemption."

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
Access and Correction: Users should have qualified access personal data that they have provided, and to rectify, complete, amend, or delete this data.	Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's designated record set. The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given	

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
	the right to have such denials reviewed by a licensed health care professional for a second opinion. Covered entities may impose reasonable, cost-based fees for the cost of copying and postage. The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of	

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
	notice to amend from another covered entity.	
Risk Management: Users should expect organizations to take steps to manage and/or mitigate the risk of harmful uses or exposure of personal data.	A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule. A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices. A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule. A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its	

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
	workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.	
Accountability: Organizations should be accountable externally and within their own processes for the use of personal information collected, maintained, and used in their systems.	The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing these standards and may conduct complaint investigations and compliance reviews. Consistent with the principles for achieving compliance provided in the Privacy Rule, OCR will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Privacy Rule. Covered entities that fail to comply voluntarily with the standards may be subject to civil money penalties. In addition, certain violations of the Privacy Rule may be subject to criminal prosecution.	Each institution engaged in research that is covered by this policy, with the exception of research eligible for exemption under §46.104, and that is conducted or supported by a Federal department or agency, shall provide written assurance satisfactory to the department or agency head that it will comply with the requirements of this policy. In lieu of requiring submission of an assurance, individual department or agency heads shall accept the existence of a current assurance, appropriate for the research in question, on file with the Office for Human Research Protections, HHS, or any successor office, and approved for Federal-wide use by that office. When the existence of an HHS-approved assurance is accepted in lieu of requiring submission of an assurance, reports (except certification) required by this policy to be made to department and agency heads shall also be made to the Office for Human Research Protections, HHS, or any successor office. Federal

NTIA RFC Privacy Outcomes	HIPAA Privacy Rule	Revised Common Rule
		departments and agencies will conduct or support research covered by this policy only if the institution has provided an assurance that it will comply with the requirements of this policy, as provided in this section, and only if the institution has certified to the department or agency head that the research has been reviewed and approved by an IRB (if such certification is required by §46.103(d)).