December 16, 2019

The Honorable Diana DeGette  
US House of Representatives  
2111 Rayburn House Office Building  
Washington, DC 20515

The Honorable Fred Upton  
US House of Representatives  
2183 Rayburn House Office Building  
Washington, DC 20515

Submitted electronically: cures2@mail.house.gov

Re: Cures 2.0

Dear Representatives DeGette and Upton,

The American Medical Informatics Association (AMIA) appreciates the opportunity to provide input on “Cures 2.0.”

Informatics is the science of how to use data, information, and knowledge to improve human health and the delivery of health care services. 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. AMIA members advance health and wellness by implementing and evaluating informatics interventions, innovations, and public policy across settings and patient populations, adding to our collective understanding of health in the 21st century through peer-reviewed journals and scientific meetings.

AMIA was a strong supporter of the 21st Century Cures Act of 2016, and the informatics community contributed directly to numerous provisions in the landmark legislation. A report that AMIA published in the *Journal of the American Medical Informatics Association* in June 2015 offered numerous recommendations for how to address many health information technology (IT) challenges from a wide range of perspectives.1 AMIA’s *EHR 2020 Task Force Report* would go on to serve as a rubric for a series of hearings held by the Senate HELP Committee in 2015 and 2016.2

The Cures Act established an ambitious agenda for how EHRs must evolve to deliver on the many as-yet-undelivered promises first described nearly a decade ago in the HITECH Act.3 Among these ambitious changes was a new statutory definition of “interoperability,” in the context of health IT

---


that: (1) enables the secure exchange and use of electronic health information without special effort on the part of the user; (2) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and (3) does not constitute information blocking.4 Added to this comprehensive definition was a new adjunct to ONC’s Certification Program that outlines specific conditions for and maintenance of Certification. One such condition is that certified health IT have “published application programming interfaces and allows health information from such technology to be accessed, exchanged, and used without special effort…including providing access to all data elements of a patient’s electronic health record…”5

As strong supporters of the 21st Century Cures Act of 2016, we are gratified to see members of Congress thinking ahead about how to build on this vital legislation. **However, we first recommend that members of the Energy & Commerce Committee understand how the Administration is implementing the Cures Act and whether adjustments in implementation or oversight are needed.** The Cures Act is vast, and the provisions established in Section 4000, for example, have not yet been finalized, nearly three years after passage. As part of the fact-finding for Cures 2.0, AMIA encourages your offices to identify what key provisions are still in development and better understand how Cures 1.0 is being implemented.

In reviewing your agenda for Cures 2.0, we are especially supportive of your intended focus areas of digital health and “how to harness data to empower patients and improve their health.” As our nation’s healthcare delivery system continues its digital transformation, we note the heightened interest from consumer technology companies in health. Major technology companies and major retail stores are investing heavily in digital health tools and are working to leverage new troves of data to better understand patients’ picture of health.

This blurring of clinical and consumer technologies brings both promise and opportunity for improving Americans’ health and wellness, as well as increases risks to privacy and safety. Most acutely for Congress, there is a lack of consumer protection for health data beyond the HIPAA-regulated environment and there is a lack of evidentiary standards for digital health tools and mobile applications. While we anticipate that Cures 2.0 could include a host of important policy tweaks and updates, we encourage the Committee to think centrally about how to ensure safety in our fast-approaching future dominated by innovations in artificial intelligence, big data aggregation, and advances in biotechnology.

Below in the enclosed attachment, we offer several areas for the Committee to consider as it undertakes a landscape review for Cures 2.0, including:

- Establishing Consumer Protections for Health Data Privacy
- Breaking Down Data Silos Funded by the NIH
- Modernizing Regulation of Software that Performs Medical Device Functions
- Focusing on Health Data Standards Research & Development
- Enabling Innovation and Research within HIPAA-Protected Environments

---

4 Section 4003 of 21st Century Cures Act
5 Section 4002 of 21st Century Cures Act
• Improving Patient Safety and Security with Unique Patient Identifiers

We hope our comments are helpful as you gather more information on potential legislation and as we advance towards the shared goal of utilizing informatics to improve health care. Should you have questions about these comments or require additional information, please contact Jeffery Smith, Vice President of Public Policy at jsmith@amia.org or (301) 657-1291. We look forward to continued partnership and dialogue.

Sincerely,

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

(Enclosed: AMIA Response to Cures 2.0 Request for Comment)
Establishing Consumer Protections for Health Data Privacy

Two major trends necessitate Congressional action on health data privacy: (1) The volume, variety, and velocity of health data are rapidly growing across care delivery, research, and commercial settings, and (2) the line between consumer and health information systems and devices continues to blur. Together with rules in development by the Office of the National Coordinator for Health Information Technology (ONC), these trends will position patients as mediums to a vast, yet nascent ecosystem of clinician-, researcher- and patient-facing apps, which will rely on new-found access to data produced and retained by certified health IT.6

When this future is viewed alongside the current reality of scant consumer protections outside the HIPAA-regulated environment, the goal espoused by Cures to provide patients access to their data via APIs “without special effort,” has the real and significant potential to create privacy risks and opportunities for fraud.7-8 The challenges posed to privacy, fraud, and abuse in the near-term API-driven future will require that Congress acts to fill the consumer protection gaps residing just beyond the reach of HIPAA8 – either now, as part of ongoing consumer data protection legislation discussions, or at some point after more demonstrable harm is committed against Medicare and Medicaid beneficiaries and other patients who erroneously believe that their data is protected from misuse.9,10

Specifically, we urge Congress to pursue updated privacy policies that lays a foundation for (1) individual data rights; (2) obligations and custodial duties for data owners and processors; and (3) data use prohibitions across jurisdictional and geographic boundaries, while also establishing a process for jurisdictions to address local needs and norms. We must strive for both harmony in how privacy is protected, and autonomy promoted, regardless of whether such data is held by a Covered Entity, Business Associate, or Commercial entity. A forthcoming set of AMIA policy principles and position statements will add definition to how the wider health informatics community recommends we proceed with health data privacy and we will be happy to share those once they are public.

---

6 Farr C. Health care is one of Apple's most lucrative opportunities: Morgan Stanley. CNBC
8 Grundy, Chiu. et al. sought to understand how user data are shared by top rated medicines related mobile applications (apps) and to characterize privacy risks to app users, both clinicians and consumers. They found that sharing of user data is routine, yet far from transparent. 79% of sampled apps shared user data and 55 unique entities, owned by 46 parent companies, received or processed app user data, including developers and parent companies (and service providers. Grundy Q, Chiu K. et al. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ 2019;364:l920 https://www.bmj.com/content/364/bmj.l920
Breaking Down Data Silos Funded by the NIH

The NIH recently released an updated draft of its Policy for Data Management and Sharing. Commenting on its initial draft in 2017, AMIA articulated areas where major revisions and edits would help improve the NIH’s goal of improving the findability, accessibility, interoperability, and reusability of NIH-funded scientific data. Specifically, we recommended that data management and sharing plans play a more central role in the overall project evaluation by being scorable elements of grant proposals. This would position data management and sharing as part of the science, rather than a regulatory burden. Given our national investments in data-driven discovery, and the NIH’s own Data Science Strategy, elevating data management and sharing plans as scorable elements of grants is critical.

Unfortunately, the NIH released an updated version of its draft policy in November 2019 and we are deeply concerned that this policy will perpetuate, not mediate, a proliferation of data silos across the regulated clinical and academic research landscape funded by the NIH. Rather than leverage its authority to establish policy that would greatly improve data management and sharing practices, the NIH seems poised to finalize a laissez faire policy that would simply require a plan be developed on a “just-in-time” basis and reviewable by program staff – not subject matter experts. This approach will undoubtedly hinder access to and use of taxpayer-funded scientific data and reinforce data silos at a time when we should have national leadership from the NIH. We recommend that the Committee monitor this issue closely and be prepared to act legislatively through Cures 2.0, if necessary.

Modernizing Regulation of Software that Performs Medical Device Functions

FDA is currently testing a new regulatory framework for Software-as-a-Medical Device (SaMD) as part of the Precertification (Pre-Cert) Program. This new regulatory framework is proposing to focus on regulating firms and developers, rather than products. While we are overall supportive of the pilot’s goal, we believe that the FDA would benefit from additional authority to carry out such a regulatory paradigm. Recent inquiries from other members of Congress have highlighted the need to enshrine this authority in statute. Doing so would also provide Congress additional oversight over the program, as well as opportunities to set requirements, such as those around post-market surveillance and real-world performance.

Focusing on Health Data Standards Research & Development

Through the efforts of ONC and its Health IT Certification Program, the private sector-led development of data standards has accelerated, especially standards related to HL7’s Fast Healthcare Interoperability Resources (FHIR). While clinical data standards development has evolved and

---


matured, there is a growing amount of data generated outside the traditional EHR context – including medical device data, remote sensors, and social determinants of health (SDoH) data. Given the need to look beyond EHR data interoperability to remote monitoring and medical devices, Cures 2.0 should support private sector-led research and development of data standards across these other sources.

**Enabling Innovation and Research within HIPAA-Protected Environments**

Following the widespread implementation of EHRs, the potential of such data in a secure manner to improve care through data analytics has never been greater. Indeed, recouping substantial value from our national investment in EHRs can only be expected if greater access to such data is available. HR 6, Rep. Upton’s bill that passed the House of Representatives in 2015, includes a number of provisions focused on “accessing, sharing, and using health data for research purposes.” One such provision is the use of health data for research purposes within the definition of HIPAA “health care operations.”

At present, “health care operations” under HIPAA excludes studies whose “primary purpose” includes the “obtaining of generalizable knowledge,” or improvements of care beyond the institution or organization. This thus prevents the sharing of knowledge to increase value-based care across healthcare. This status quo has further resulted in data silos that are important reservoirs for care improvements for both individual patients and populations. In an era of ubiquitous EHRs, this language is a major impediment to a transformation to value-based care. Changing this regulation would offer the same degree of privacy protection as in the past, while allowing data research to transform our healthcare system.

**Improving Patient Safety and Security with Unique Patient Identifiers**

For nearly two decades, innovation and industry progress has been stifled due to a ban on using federal funds to promulgate or adopt a national patient identifier. Further, without the ability of clinicians to correctly connect a patient with their medical record, lives have been lost and medical errors have needlessly occurred. These are situations that could have been avoidable had patients been able to have been accurately identified and matched with their records. This problem is so dire that one of the nation’s leading patient safety organizations, the ECRI Institute, named patient misidentification among the top ten threats to patient safety. Removing the statutory prohibition will provide HHS the ability to evaluate a range of patient identification solutions and enable it to work with the private sector to explore potential challenges and identify a solution that protects patient privacy and is cost-effective, scalable, and secure.

---

16 [https://www.ecri.org/EmailResources/PSRO/Top10/2017_PSTop10_ExecutiveBrief.pdf](https://www.ecri.org/EmailResources/PSRO/Top10/2017_PSTop10_ExecutiveBrief.pdf)