

**Senate Committee on Health, Education, Labor and Pensions**

**United States Senate**

**Statement of**

**Donald Rucker, M.D.**

**National Coordinator for Health Information Technology**

**Office of the National Coordinator for Health IT**

**Department of Health and Human Services**

**May 7, 2019**

Chairman Alexander, Ranking Member Murray, distinguished Members of the Committee, thank you for the opportunity to testify in support of the Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology's (ONC) efforts to implement provisions of title IV of the 21<sup>st</sup> Century Cures Act (Cures Act). I want to thank Congress and this Committee for your shared commitment to stimulate a modern and connected health care system. The bipartisan Cures Act accelerates our efforts to ensure that patients' records follow them when and where they need them.

The Cures Act directs the HHS Secretary to adopt standards and policies that advance the seamless and secure flow of electronic health information (EHI) across the health system. On March 4, 2019, ONC issued a proposed rule to implement key provisions in title IV of the Cures Act. This proposed rule aims to drive the electronic access, exchange, and use of health information. It seeks to inject competition into the health care delivery system by addressing both technical barriers and business practices that impede the secure and appropriate sharing of data. A central purpose of the proposed rule is to facilitate patient access to their EHI on their smartphone, growing a nascent patient- and provider-facing app economy.

I would like to begin by discussing the current health care and health information technology (health IT) environments. In an extraordinary shift from a decade ago, most hospitals and providers now use electronic health records (EHR).<sup>1</sup> However, information captured in these systems often remains inaccessible to patients and to their providers across different settings.

Fragmented care can lead to hospital readmissions, medical errors, and poor health outcomes, especially among patients with multiple chronic conditions who rely on coordinated care to help manage their health.<sup>2, 3, 4</sup> Today, only half of hospitals report having the necessary information electronically available from outside providers or sources at the point of care. Notably, hospitals with advanced interoperability capabilities are significantly more likely to have information available from outside sources compared with hospitals lacking those capabilities.<sup>5</sup> A health system where information flows appropriately and securely to patients and their providers can improve care coordination, reduce adverse events, and lower costs. ONC designed this proposed rule to help stimulate a more connected health system that leverages health information to better serve patients.

To develop this proposed rule, ONC coordinated extensively with relevant federal agencies. We also met with more than 150 external stakeholders from across the health system to improve our understanding of the on-the-ground needs and barriers related to the flow of EHI. While the proposed rule covers many provisions within title IV of the Cures Act, today, I am going to highlight how the proposed rule addresses the Conditions of Certification and Information Blocking provisions.

The conditions and maintenance of certification proposals include requirements for health IT developers under the ONC Health IT Certification Program and cover a range of business practices and behaviors that impede the access, exchange, and use of EHI. The first condition I will highlight focuses on the Cures Act requirement for health IT developers to publish

application programming interfaces (APIs) that allow health information to be securely accessed, exchanged, and used “without special effort.” Requiring health IT developers to publish an API is not enough. Without common standards, third-party app developers need to learn and use different requirements and database structures for each health IT system. This hampers competition by binding patients and app developers to particular clinicians or products.

The proposed rule includes a suite of proposals that focus on certified health IT developers making available secure, standards-based APIs that facilitate patients’ use of their smartphones (or other mobile devices) for accessing EHI at no cost. It also supports clinicians’ ability to partner with third-party software developers offering unique and competitive services that support patient care. Specifically, ONC proposes to adopt a new standards-based API certification criterion that would require that a health IT product support “read” access to health information for both a single patient and for a group of patients. The proposed rule addresses the Cures Act phrase “without special effort” through a number of proposals that promote standardized, transparent, and pro-competitive market practices. Once finalized, health care providers would have two years from the final rule’s publication date to offer patients’ access to their EHI through secure, standards-based APIs.

While developing the proposed rule, stakeholders shared two overarching security concerns. The first concern has to do with the overall security of APIs. The second concern touches upon the secondary use of data. When it comes to security, it is important to note that the health IT developers and health care providers using certified health IT would deploy APIs with the same security measures used by other industries, such as banking (through the OAuth 2 standard). In fact, health care providers already offer the same security measures to protect patient portals. Third-party health care apps who wish to connect to a health IT developer’s certified API would need to establish secure connections, prompt patients to authenticate themselves to their health care provider, and obtain a patient’s approval on the scope of data that the app may access.

How data is secured and used once in third-party apps illustrates a pressing issue that is currently part of a national discussion a discussion that extends beyond health care and into data privacy, stewardship, and regulatory interventions. How APIs secure their connections and follow patients’ individual preferences in health care is no exception. Many third-party apps are not required to implement the privacy protections and patient rights of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, but they may be subject to the Federal Trade Commission (FTC) jurisdiction, including the Health Breach Notification Rule.

The HHS Office for Civil Rights (OCR) has regulatory authority to ensure the privacy and security of data applies only to HIPAA covered entities (e.g., many health care providers, health plans) and their business associates (e.g., EHR developers). In April 2019, OCR released new frequently asked questions (FAQs) about the HIPAA right of access related to patient-designated apps and APIs. The FAQs clarify that once protected health information has been shared to a third-party app, as directed by the individual, the HIPAA-covered entity (or its business associate that fulfills the access request on behalf of the covered entity) will not be liable under HIPAA for

subsequent use or disclosure of that particular electronic protected health information. This is provided that, with respect to the app, the app developer is not itself a business associate of a covered entity, directly or through another business associate.

Across all business sectors, individuals often have little say with respect to the secondary use and disclosure of their personal data. However, the misuse of health information can have lifelong consequences for the patient. Individuals should balance their selection and use of a health app with the potential risk of having negative implications. These risks are similar to when they enter sensitive health data into an online search, contribute their DNA to learn about their ancestral heritage, share their credit card information when making an online purchase, or consent to location services on their phones. It is important to note that deeply sensitive health facts about patients can be inferred from consumer data “exhaust” such as accelerometers, location services, and a wide variety of app and social media usage patterns.

Individuals should have the ability to decide whether the potential benefit of an app to manage their health care information and medical conditions outweighs potential risks. This should be the patient’s choice. Interestingly, some entities advocating to protect the patient from inappropriate secondary uses and disclosures of the patient’s data have business models at risk from patients accessing their EHI. ONC’s proposed rule empowers individuals to electronically access and share their EHI, enabling an individual’s HIPAA right of access, and affording the patient agency over their own health information that is often absent in health care.

Today’s fragmented health system forces individuals or caregivers to navigate a byzantine system to manage their care. Emerging technologies and the use of mobile apps will provide individuals with access to their own EHI that can follow them across providers and health plans, and advance an app marketplace that addresses unique patient needs.<sup>6</sup> For instance, an app may empower patients with multiple chronic conditions to consolidate and share their care journey with each clinician they visit, potentially preventing adverse and life-threatening events due to missing clinical information. A robust health app ecosystem can also lead to the development of disease-specific apps that allow patients to choose whether to share their health information with researchers working on clinical trials to test a drug or treatment’s efficacy like those in the National Institutes of Health’s *All of Us* Research Program. Apps could also help address barriers related to access by presenting complex information in easy to understand ways.

We have seen promising signs of this occurring in the private sector. Last year, Apple introduced their Health Records on the iPhone using the same modern computing standards included in our proposed rule. A little over a year later, over 200 health institutions use the Health app to offer their patients access to their health records. Many other entrepreneurs are developing novel health apps as well, and our proposed rule is designed to lower the barriers to their entry into the health app industry. Later, I will discuss how we can envision this same approach taking shape when it comes to price transparency and providing patients with the ability to shop for care based on the price and quality of care.

In addition to addressing the flow of EHI, this proposed rule seeks to enhance the safety of health IT. In 1999, when most clinicians were still using paper records, the former Institute of Medicine (now the National Academy of Medicine) published a seminal report, to *Err is Human*, where they estimated that between 44,000 to 98,000 people die in hospitals each year due to preventable medical errors.<sup>7</sup> There is ample evidence that well-designed health IT systems can make care safer.<sup>8</sup> However, due to the innate complexity of medicine and radical changes to established clinical workflows, health IT has introduced new safety issues and also exacerbated others.

One resounding complaint we heard from the patient safety community is that health IT developers use gag clauses to inhibit the flow of essential information that could improve safety across systems. A 2012 National Academy of Medicine report found that such clauses discourage users from sharing information about patient safety risks, significantly limiting the ability of users to understand how health IT products impact patient safety. The report stressed the need for health IT developers to enable the exchange of information regarding user experiences, including the sharing of screenshots.<sup>9</sup> As part of ONC's patient safety efforts that are paramount to its mission, programs, and policies, this proposed rule would prevent certified health IT developers from prohibiting or restricting communications regarding usability, interoperability, security, user experiences, business practices, and technology use. We also included provisions to respect health IT developers' intellectual property in the software.

The promise of standards-based API technology can only be successful if current business practices that enable information blocking to occur are dismantled. For that reason, I thank Congress for establishing consequences for information blocking in the Cures Act. The information blocking provisions were enacted in response to concerns that some individuals and entities engage in practices that unreasonably limit the availability and use of EHI for authorized and permitted purposes. These practices undermine public and private sector investments in the nation's health IT infrastructure. They also frustrate efforts to use modern technologies to improve health care quality and efficiency, accelerate research and innovation, and provide greater value and choice to health care consumers.

The information blocking provisions apply to health care providers, developers of certified health IT, health information exchanges, and health information networks. Under the Cures Act, the HHS Office of the Inspector General (OIG) has authority to investigate information blocking claims against these entities. Health care providers can be subject to disincentives determined by the HHS Secretary if the OIG finds that the provider has knowingly and unreasonably engaged in information blocking. Developers of certified health IT, health information exchanges, and health information networks can be subject to civil monetary penalties determined by OIG of up to \$1 million per violation.

The proposed rule establishes seven exceptions that identify certain reasonable and necessary activities that do not constitute information blocking. To develop the proposed exceptions, we were guided by three overarching policy considerations. First, the exceptions would be limited to certain activities that clearly advance the aims of the information blocking provision. Second,

each exception is intended to address a significant risk that regulated actors (i.e., health care providers, health IT developers of certified health IT, health information networks, and health information exchanges) would not engage in certain reasonable and necessary activities because of potential uncertainty regarding whether those activities would be considered information blocking. Third, each exception would be tailored, through appropriate conditions, so that it is limited to those reasonable and necessary activities that it is designed to exempt. These exceptions also would be subject to strict conditions to ensure that they do not extend protections to practices that should be considered information blocking.

An action would not be treated as information blocking if it satisfies one or more of these seven exceptions. The first three exceptions extend to certain activities that are reasonable and necessary to prevent harm to patients and others; promote the privacy of EHI; and promote the security of EHI. We believe that without these exceptions, it would erode trust and undermine efforts to provide access and facilitate the exchange and use of EHI for important purposes.

The next three exceptions promote competition and innovation. First, we propose to permit the recovery of certain types of reasonable costs incurred to provide technology and services that enable access to EHI and facilitate the exchange and use of that information. For example, this exception enables the recovery of costs reasonably incurred to develop technologies and provide services that enhance interoperability, while not protecting rent-seeking, opportunistic fees, and exclusionary practices that interfere with access, exchange, and use of EHI. Second, the proposed rule would permit an entity to decline infeasible requests to exchange EHI but would still require the actor to find a reasonable alternative for providing the EHI. Third, we propose an exception that would permit the licensing of interoperability elements on reasonable and non-discriminatory terms. Contractual and intellectual property rights are frequently used to extract rents for access to EHI or to prevent competition from developers of interoperable technologies and services. Such practices frustrate interoperability and stifle competition and innovation. In many scenarios, however, it is generally appropriate to license intellectual property on reasonable and non-discriminatory terms to support access, exchange, and use of EHI. This exception would further the goals of the information blocking provision by allowing for the protection of the value of their innovations and earn returns on the investments made to develop, maintain, and update those innovations.

For health IT to perform properly and efficiently, it must be maintained, and in some instances improved. This may require that health IT be taken offline temporarily. The final exception would allow EHI to be temporarily unavailable during health IT implementation upgrades, repairs, and other changes.

ONC's proposed rule primarily focuses on clinical data. However, advances in computer science and the maturity of data standards are accelerating the convergence of medical data with billing and price data. As such, the rule proposes to include such information as part of a patient's EHI that should be available for access, exchange, and use. The idiosyncratic and complex nature of pricing within the health care system has decreased efficiency and negatively impacted patients, clinicians, health systems, plans, plan sponsors, and other stakeholders.

In our current health system, there is an asymmetry of information for patients. They have few ways if any to anticipate or plan for costs, lower or compare costs, and, importantly, measure their quality of care or coverage relative to the price they pay. Transparency in the price and cost of health care could help address some of those concerns by empowering patients with information they need to make informed decisions. Further, the wide availability of price information for health care services could engender competition and accountability based on the quality and value of those services in health care. Increased consumer demand, aligned incentives, more accessible and digestible information, and the evolution of price transparency tools are critical components to move from a delivery system that rewards volume of services to one that recognizes and rewards the value of health care services.

Unfortunately, the complex and decentralized nature of how payment information for health care services is currently created, structured, and stored presents many challenges to achieving price transparency. This entire information chain is geared to retrospective payments rather than prices. The public has little idea what the CPT billing codes mean, or how they might be combined if at all to determine a prospective price. As noted in my discussion of APIs, we can see a future where, for example, platforms use raw data to provide consumers with digestible price information through their preferred medium such as an online tool or smartphone app. As such, the proposed rule seeks public input on both how we can scope and capture price information as part of EHI as well as what steps HHS can take, using all its available resources, to provide price transparency.

I also want to note that, as part of ONC's implementation of Congressional direction articulated through the Cures Act, we recently issued an updated draft of the Trusted Exchange Framework and Common Agreement (TEFCA) for public comment, which includes a common set of principles that facilitate trust between health information networks. The TEFCA is designed to provide a single "on-ramp" to nationwide connectivity and advance a landscape where information securely follows the patient where and when it is needed. We also issued a funding opportunity announcement for the selection of a private sector non-profit organization that will serve as the Recognized Coordinating Entity responsible for developing, updating, implementing, and maintaining the Common Agreement with ONC. This Common Agreement will create the baseline technical and legal requirements for networks to share EHI across the nation. Nationwide interoperability is not a simple undertaking, and something as expansive as a final TEFCA requires thoughtful consideration of the issues and challenges. ONC's intention with releasing the draft for a second round of public comment is to ensure we get it right.

I also wanted to note that a significant unmet need in the health care system is for patients with behavioral health conditions. These patients may transition between emergency rooms, primary care, mental and behavioral health specialists, shelters, group homes, and various treatment centers. When these patients present at a new setting, a provider may know where they transferred from, but lack the necessary insight about their care journey. ONC previously funded various programs to accelerate health information exchange at the state, regional, and local level. These community information exchanges have demonstrated reductions in care utilization, such as through reduced duplicate testing and imaging for patients.<sup>10, 11</sup> Community information

exchanges are positioned to connect patients with clinical services and social supports. ONC remains committed to advancing community information exchange to support care coordination and improve health, especially for patients with behavioral health conditions.

In addition, the provisions in our proposed rule to support the use of secure APIs and to support the access, exchange, and use of electronic health information can also offer promising strategies to combat opioid use disorder (OUD). Data such as opioid prescription drug data, prior OUD diagnosis and treatment data, and community health information is essential for providers to be able to prevent and treat OUD. This data continues to be siloed across systems. This makes access to this information and to related decision-making tools burdensome for providers. We look forward to continuing to advance the adoption of common industry standards that could help to address opioid use disorder prevention and treatment while addressing the patients' need for privacy.

In summary, much of today's American health care delivery system remains complex and opaque to providers and patients. Congress's 21st Century Cures Act and advances in modern computing allow us to revisit many of the assumptions about what delivery of medical care could and should be. ONC's proposed rule and advancements on the Trusted Exchange Framework and Common Agreement serve as major steps to make health care more transparent, accountable, and patient and provider accessible. We believe these policies firmly place the nation on the path to achieving the long-term benefits of interoperability of electronic health information connecting for the U.S. health system.

We will continue to keep Congress informed of milestones as they occur. Mr. Chairman, Ranking Member, and Members of the Committee, thank you for the opportunity to testify. I look forward to responding to any questions you may have.



## Sources

---

- <sup>1</sup> Office of the National Coordinator for Health Information Technology (2018). *Report to Congress: Annual Update on the Adoption of a Nationwide System for Electronic Use and Exchange of Health Information*. [online] Washington, DC. Available at: <https://www.healthit.gov/sites/default/files/page/2018-12/2018-HITECH-report-to-congress.pdf> [Accessed 25 Apr. 2019].
- <sup>2</sup> Moore, Carlton et al. "Medical Errors Related To Discontinuity of Care From An Inpatient To An Outpatient Setting." *Journal Of General Internal Medicine*, vol 18, no. 8, 2003, pp. 646-651. *Springer Nature*, doi:10.1046/j.1525-1497.2003.20722.x. Accessed 25 Apr 2019.
- <sup>3</sup> Tsai TC., Orav EJ., & Jha AK. "Care Fragmentation in the Postdischarge Period: Surgical Readmissions, Distance of Travel, and Postoperative Mortality." *JAMA Surg*. 2015 Jan;150(1):59-64. Accessed 25 Apr 2019.
- <sup>4</sup> Robert Wood Johnson Foundation (U.S.) *The Revolving Door: A Report on U.S. Hospital Readmissions*. The Dartmouth Institute for Health Policy and Clinical Practice, 2013.
- <sup>5</sup> Pylypchuk Y., Johnson C., Henry J. & Ciricean D. (November 2018). "Variation in Interoperability among U.S. Non-federal Acute Care Hospitals in 2017." *ONC Data Brief*, no.42. Office of the National Coordinator for Health Information Technology: Washington DC.
- <sup>6</sup> Mandl, Kenneth D., Mandel Joshua C., & Kohane Isaac S. "Driving Innovation in Health Systems through an Apps-Based Information Economy." *Cell Systems*. 2015 Jul;1(1):8-13. Accessed 25 Apr 2019.
- <sup>7</sup> Institute of Medicine. 2000. *To Err Is Human: Building a Safer Health System*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/9728>.
- <sup>8</sup> Office of the National Coordinator for Health Information Technology. "Effects of Meaningful Use Functionalities On Health Care Quality, Safety, And Efficiency." *Dashboard.Healthit.Gov*, 2014, <https://dashboard.healthit.gov/quickstats/pages/FIG-Health-IT-Literature-Review-Infographic.php>.
- <sup>9</sup> Institute of Medicine (U. S.). *Health IT and Patient Safety: Building Safer Systems For Better Care (Health Information Technology And Patient Safety)*. National Academies Press, 2012.
- <sup>10</sup> Ayer, Turgay et al. "The Impact of Health Information Exchanges on Emergency Department Length Of Stay." *Production and Operations Management*, vol 28, no. 3, 2018, pp. 740-758. *Wiley*, doi:10.1111/poms.12953. Accessed 25 Apr 2019.
- <sup>11</sup> Lammers, Eric J. et al. "Does Health Information Exchange Reduce Redundant Imaging? Evidence from Emergency Departments." *Medical Care*, vol 52, no. 3, 2014, pp. 227-234. *Ovid Technologies (Wolters Kluwer Health)*, doi:10.1097/mlr.0000000000000067. Accessed 25 Apr 2019.