May 16, 2019

Donald Rucker, M.D.
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C St. SW, Floor 7
Mary Switzer Building
Washington, DC 20201

Submitted electronically via: http://www.regulations.gov

RE: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Dear Dr. Rucker,

OCHIN applauds the Office of the National Coordinator for Health Information Technology's (ONC's) extensive work to address data blocking of electronic health information exchange. OCHIN appreciates the opportunity to submit comments on the ONC's proposed rule, the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program*.

OCHIN is a 501(c)(3) not-for-profit community-based health information technology (HIT) collaborative based in Portland, Oregon. Our collaborative supports health care providers that are treating the nation's most vulnerable patients. This population, and the providers who serve them, are underrepresented in the data sharing and data blocking conversation. OCHIN helps elevate health information exchange and health IT for a large percentage of patients who are being treated by safety net providers across the nation. Our goal is to provide a national voice for safety net providers within health care technology and health care information exchange.

As a national network that supports over 500 health centers across the country, OCHIN scales health IT services through hosted electronic health records (EHRs), telehealth services, and other professional services to our members. To provide the highest level of care to this unique patient population, OCHIN has grown to be one of the largest movers of health data in the nation. Since 2010 we have shared over 76 million clinical summaries, and we continue to innovate within health information exchange and expand our partnerships to improve care coordination for especially complex and vulnerable patients.

In addition to serving health centers that provide care to vulnerable patients, we operate as a learning collaborative, researching issues impacting safety net patients and providers. Our research team has extensively studied the opioid crisis, the deployment of electronic health records into community health centers, practice transformation, interventional strategies, HIV and infectious disease, social determinants of health, mental health, and obesity, among other topics impacting the health of vulnerable

populations. We are one of the 13 PCORnet designated research sites, and one of the few entities engaging in national research on issues specifically impacting the safety net population.

OCHIN's Summary of Comments on the ONC Proposed Information Blocking Rule:

OCHIN strongly agrees with the goal of interoperability for treatment purposes and improved care coordination. Improving data movement between health care providers is paramount to achieving this goal. This long-awaited Rule, if inclusive of all health care providers across the nation, will undoubtedly improve patient outcomes and public health overall.

While the goal of the Information Blocking Rule is supported by OCHIN, we urge caution and encourage ONC to slow the trajectory of this Rule. The ONC is moving too quickly to fully assess and field the extensive issues that will inevitably arise, putting patients and providers at risk and health information exchanges (HIEs) in a position of liability. OCHIN does not believe there are appropriate protections for patients, providers, or HIEs outlined within. Additionally, OCHIN believes without substantial additional time to implement, this Rule will add significant financial burden to already stretched health centers and small practices.

OCHIN is also concerned about the overall liability placed upon the provider as an "actor" to prevent harm. Small safety net clinics and providers do not have the capital resources or the human resource bandwidth to undertake such liability. Many of these entities do not have the expertise available to implement necessary operational policies or navigate complicated business agreements for data exchange with covered and non-covered entities, and acquiring this guidance is a substantial investment.

Finally, HIPAA covered entities and their business associates are subject to strict legal constraints and controls, and for good reason. We are concerned about the consequences of this free flow of data from a regulated environment to a non-regulated environment, and how non-HIPAA covered entities may utilize this sensitive information, especially for patients within the safety net with more acute complications and social complexities than the general public. As an entity that speaks for the safety net, we believe this is a grave concern that must be addressed before the consequences disproportionately impact the vulnerable population and the providers serving them. Privacy should not become a luxury.

A. Information Blocking

a. Provider Protections

Interoperability is critical for treatment. The premise of the ONC rule is that patients can own and direct their data. However, there must be provider safeguards and safe harbors in place to protect the transfer of data from a HIPAA regulated environment to a non-HIPAA regulated environment. Health care providers are required to adhere to HIPAA laws. A safeguard must be codified in statute to ensure liability is attached to the entity that misuses the data without the consent of the patient. We strongly believe this Rule is the making of a two-tiered system, with only half of the players subject to HIPAA. There seems little justification for allowing some entities to be covered and others not.

The solution is to make every entity that transfers or receives patient protected health information (PHI) a covered entity or otherwise comply with HIPAA and HITECH, as well as the 21st Century Cures Act. This would hold all actors that receive protected health information to the same standards as other entities handling such private and valuable information. If an entity can be harshly penalized for

preventing the movement of patient data, similar requirements must hold those at every level receiving PHI to be independently liable for their actions.

OCHIN is aware of the recent guidance by HHS that releases liability from the covered entity once the health information is transferred to an uncovered entity. A simple guidance does not provide the security necessary to allow for unrestricted data movement with such extraordinary risks involved. There must be an explicit statutory release of liability or safe harbor for the release of PHI. ONC must take this into consideration and delay implementation of this Rule until liability release is written into statute, and proper restrictions for use of data can be placed on app developers and other uncovered entities that gain access to health data.

HIPAA was created to protect health data integrity, confidentiality, and availability. Health care data is the number one target for hacking, which could result in identity theft, bias or discrimination, or blackmail. Should these non-covered entities sell health data or get hacked, it will not be the app that is blamed for the release of PHI but rather, the provider at the point of collection. Health care providers and health IT vendors may not have the bandwidth or capability to vet app developers and operators to ensure they are responsible actors. Without this statutory language, the provider at the point of collection can likely expect to face with lawsuits, which could devastate small or rural entities. The HHS Guidance does not have the legal clarity to rebuke possible lawsuits, and will still result in unnecessary legal hardship for entities with minimal operating margins.

Requiring all organizations to enact their own internal policies of how to comply with this Rule puts substantial burden on the small and rural providers. Many of the directions outlined within are aimed at large health organizations that have internal systems and support to handle legal and policy matters. The requirement for all health organizations to sign onto agreements for data transfer with uncovered entities overlooks the small and rural providers without such resources or the ability to affordably outsource these needs. It is foreseeable that providers may sign onto contracts that result in them undertaking extensive liability.

OCHIN suggests ONC or HHS financially support health centers treating vulnerable patients for navigating these issues, the application of which could be based on the staffing level, rural classification, or number of patients within the safety net. Without this additional support, safety net providers who are vital to the nation's overall public health, are being placed in a precarious position. With such tight resources, they may be forced to choose between providing care or investing in legal assistance. Additionally, ONC must be thoughtful in the application of the standards outlined in this Rule and make contract navigation simple by ensuring financial support is available to protect the nation's safety net providers from this liability.

b. Patient Protections

Patients require and deserve protection against those phishing for valuable medical information for non-medical purposes, especially vulnerable patients such as seniors and those within the safety net. These protections must include rules that apply to non-HIPAA entities, a prevention on the sale of patient data, and strong transparency laws that require an app developer or other non-covered party requesting health data to disclose what they plan to do with the data prior to the patient consenting to its use.

As the health IT app ecosystem continues to evolve, patients need to be provided clear guidance and understanding of what they agree to when signing into an app and that their PHI could be at risk. Patient consent agreements must be easy to understand. These agreements for use of these apps are often in complex legalese, small text, and not available in all languages. As OCHIN supports a population that speaks 132 languages, this is a great concern to our members and their patient population.

In requiring medical data to be transferred to any application requested by a patient, the patient will likely assume that the app developer has been deemed a responsible and secure data recipient, and that their information will be kept private and not sold to third parties. This Rule does not ensure the privacy of their data. Additionally, most patient records contain some level of family history, and this information is similarly at risk of breach, further reducing the control over one's medical information. It could also share their genetic information where the patient has linked their genetic results with their EHR.

A recent BMJ article[1] exposed the high incidence of health data sharing by apps and the lack of transparency around it. This practice is entirely legal, even when done for monetary purposes as opposed to public health and research purposes. Vulnerable patients become easy targets. The study found that information shared not only included the data the user inputted into the system, but also their device name, operating system, browsing behavior, and email addresses. This makes the health data highly identifiable, and clearly violates user expectations.

Sensitive information such as mental health, substance use, or reproductive health information entered into apps currently moves with no restrictions and no transparency.[2] Under this Rule, non-HIPAA covered entities remain unrestricted in their sale of this data and are not required to have transparency as to how they use patient data. For vulnerable populations like those served by OCHIN's providers, this is especially concerning. However, the potential for health information to be used against any patient is unprecedented.

Another obstacle within the safety net community is the broad spectrum of medical literacy and level of reading comprehension. Although EHRs are quickly expanding the languages they can serve patients in, it is simply not reasonable to ask vendors to comply with all language needs in 24 months. It is even less likely the app will support patients' language needs. Beyond a potential language barrier, the terms outlined in these consent agreements are often difficult to understand, particularly for those within the safety net.

Education on patient consent is critical to ensure patients can protect themselves and advocate for their own interests. A 2018 Deloitte study showed that 91% of the population do not take the time to read terms of service, with a rate of 97% among those age 18-24.[3] If there were a financial incentive involved, this rate might be even higher. For the vulnerable population, this incentive would draw swaths of health data, which is more likely to be used against the patient, whether it be higher insurance premiums, denial

[1] Grundy Q, Chiu K, Held F, Continella A, Bero L, Holz R. Data sharing practices of medicines related apps and the mobile ecosystem; traffic, content, and network analysis. BMJ 2019;364:1920.
[2] Moglia ML, Nguyen HV, Chyjek K, Chen KT, Castaño PM. Evaluation of smartphone menstrual cycle tracking applications using an adapted APPLICATIONS scoring system. Obstet Gynecol 2016;127(6):1153-60.
[3] Obar JA, Oeldorf-Hirsch A. The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. Information, Communication, and Society 2016;1-20.

of public services, etc. OCHIN believes this may lead to further bias and disparities in the health care system against the nation's most vulnerable.

OCHIN urges ONC to appropriate additional funding for educating patients on the responsibilities and risks associated with providing apps with permission to their health data. These should come in the form of both public service announcements prior to the enactment of this rule and funds appropriated directly to health centers to educate their patients on app consent. These additional efforts could help alleviate negative impacts on patients and providers.

Finally, approvals for data sharing should not be open-ended with no term applied. Patients are likely to forget who they are sharing data with and may not be interested in continuing to data share with certain entities for an extended period.

c. Feasibility

OCHIN supports the ONC to standardize APIs. However, we believe that the 5-day response period set for data requests is unachievable. A non profit entity like OCHIN already has a difficult time with current staffing and resources to meet existing health information exchange requirements. Similar and smaller entities will likely find it challenging to ensure each of those requests are met within a timely manner under an unfunded mandate and would be hit hard by the penalties set out in the Rule. Without additional financial or staffing support, the low-margin clinics and organizations would likely be fined out of existence. This inevitably adds unnecessary costs to the system.

OCHIN would like to request the patient information request response period to be extended to 30 days for a more feasible response window. This extension would align with the standard terms of release outlined in the HHS 2014 requiring the release of lab results to patients within 30 days.[4] For small or rural entities, those operating on a tight budget, and non profit entities fielding extensive requests at once require the opportunity to respond in a timely manner, which may exceed 5 days.

Additionally, OCHIN finds the terms within the exceptions to be too ambiguous, which could result in discrepancies between the requestor and the complying entity. We are interested to know whether requests would be reviewed for their feasibility in the aggregate, as it isn't the single requests that would trigger this section, but more likely the large number of requests that would make at least the timeline infeasible to supply the necessary records. Additionally, the type or scale of request could incur prohibitive costs, or technical capabilities might render a request infeasible – concepts the ONC should consider.

d. Bidirectional Exchange

As an organization that works extensively across the nation supporting over 25 public health entities and is involved in piloting bidirectional immunization exchange directly within the EHR for safety net providers, OCHIN and our members can speak to the importance of having this capability available and unencumbered. We encourage the ONC to focus efforts as charged under Section 4005 (a) and (b) of the Cures Act specifically on interoperability as it pertains to the "bidirectional exchange" between EHRs and registries, including clinician-led clinical data registries.

[4] 42 CFR § 493

Currently, there are rural and safety net providers who participate in the immunization program via paper and fax. Until there is a national electronic system for this data, bidirectional immunization programs must be successfully implemented and funded directly by every state. Additionally, requiring these systems to run through an HIE will only add additional burden to providers. These programs should be state run, cost neutral, and bidirectional for successful outcomes. To achieve this, states should be provided additional funding to support the build out of bidirectional exchanges at the state level, and safety net providers should be financially supported to connect directly to them and supported with technical assistance to integrate data exchange within their EHRs.

B. 2015 CEHRT

a. Burden

OCHIN fully supports the removal of the 2014 Edition CEHRT from the Code of Federal Regulations. OCHIN urges the ONC to reconsider updating 2015 CEHRT standards, and instead create new 2019 CEHRT standards. This proposal breaks with ONC precedent to issue a new annual CEHRT rather than changing past CEHRT so drastically. Currently, many providers who were excluded from meaningful use have not reached compliance with 2015 CEHRT. Lack of allocated funding, the size of the practice, lack of connectivity, among other drawbacks, have left many providers behind and out of the interoperability conversation.

The proposals would place significant pressure on providers to invest in data sharing. If implemented as proposed, providers could face challenges in developing the infrastructure necessary to comply with the additional requirements. Further, the rules as proposed do not standardize the clinical vocabulary within the USCDI, which could place a burden on physician organizations to define clinical terms in a common way that will support interoperability.

The segmentation requirement also increases burden on providers. This proposed solution to protect sensitive data, such as substance use disorder history and treatment, is to segment the data to prevent it from transferring with the other requested PHI. Currently, regulatory bodies are in the process of updating 42 CFR Part 2. OCHIN suggests waiting until these processes have been completed and 42 CFR Part 2 has been updated to align with HIPAA prior to moving forward with workarounds and carveouts.

Finally, and most importantly, this software update would increase costs on safety net and community health providers, should ONC decide to move forward. Financial support and technical assistance must be provided to safety net providers. We recommend delaying the segmentation of data, and instead configuring 2019 CERHT, per ONC precedent, while the regulatory bodies perform their reformation of these sensitive data protections.

C. Research Data

OCHIN supports millions of patients with our data collaborative. The research we do is critical to understanding and improving primary care across the country. We would like to see ONC clarify for organizations that have centralized data structures the full reach of data requests, and how research entities will be impacted; specifically, those receiving funding from NIH and other research organizations for the goal of improving public health and welfare.

D. Fee Structure

The ambiguous structure and classification of cost reimbursement raises concerns. OCHIN is concerned that granular costs will increase the total cost of data exchange, and even for the largest entity, showing complete proof of costs is difficult. We are concerned this structure will lead to unintended consequences. OCHIN requests that ONC allows for a fee scale as opposed to blanket fee structure. A sliding scale structure would ensure that smaller entities would not be buried by a restrictive pricing application that threatens their operating costs, which may exist on a slim margin.

Similarly, there are fears that the subjective terms used ("reasonably," "certain," "alternative") have the potential to stifle the recovery of what would be reasonable and applicable costs, which were expended by the actor providing the service. OCHIN urges ONC to clarify the current proposal to permit the recovery of interface, administrative, maintenance, research, and delivery costs (as well as others) to avoid arbitrary complaints regarding fee structures. It would be ideal to include potential categories of reasonable costs that could be recovered to avoid misunderstandings between entities and actors after implementation of this rule, as well as a baseline for costs. Subjective terms are open to interpretation and will result in discrepancies and possible fines.

Health IT and Opioid Use Disorder Prevention and Treatment – RFI

OCHIN strongly supports the use of the Prescription Drug Monitoring Programs (PDMPs) integrated within the EHR (referred to as electronic prescribing), but with a focus on moving PDMPs to a national model as opposed to fragmented state or regional models. State boundaries paired with localized PDMPs become problematic when individuals can travel freely across state lines but health data cannot. Those with a substance use disorder can bypass the tracking system by obtaining prescriptions in two or more states.

Doctor shopping is a common issue in the opioid substance use disorder patient population.[5] Although it is recommended that patient details are entered based on a form of valid identification, it is still common that a patient is entered without a reliable reference for their basic information. This results in slightly altered entries, which prevent the patient's full prescription details from being disclosed at the time of the appointment.

With a national PDMP connected to the U.S. Department of Justice RxCheck Interstate Hub, the rules could also be standardized across the spectrum, strengthening the reach and efficiency of this program. For example, states currently vary on who is permitted to access this data. In some states, only physicians can access it, whereas the PDMP has more clout when it can be used by social workers, nurse practitioners, physician assistants, nurses, unit clerks, etc. States also vary on when this data can be used. Allowing the use of PDMP during diagnosis/assessment as opposed to solely during prescribing will give providers important data to more safely provide care for the patient as well as preventing an inappropriate prescription.

OCHIN also requests that ONC push PDMP standards for controlled substance exchange to use the NCPDP SCRIPT Medication History Request and Response transactions.[6] States' permissions for

[5] Cepeda MS, Fife D, Yuan Y, Mastrogiovanni G. Distance traveled and frequency of interstate opioid dispensing in opioid shoppers and nonshoppers. J Pain 2013;14(10):1158–1161.
[6] National Council for Prescription Drug Programs. (2019). NCPDP Standards-based Facilitator Model for PDMP.

access to a PDMP must be unified under a single national model. The disperate permissions and varied technical implementation make cross state border exchange ineffective.

It is critical that providers are able to reconcile, store, and trigger events within the EHR to support patient care. Current state models often preclude the retention of prescription data from PDMPs which reduces the effectiveness of integrating EHRs. Implementation and ongoing funding to providers is necessary both federally and from states to support the integration of PDMPs. OCHIN has shown that providers will integrate their EHRs with PDMPs if the costs of doing so are covered. By implementing a single national standard for connecting to and interacting with a PDMP that does not have variance at the state level, the medical community vendors will be able to reduce development costs and unify the user interface across their products.

We support the use of the United States Core Data Set for Interoperability, electronic prescribing, and the use of a FHIR-based API. OCHIN suggests the ONC expand electronic prescribing into a national registry, which would operate as a national prescription drug monitoring program. We currently see drawbacks of state registries when those with substance abuse disorder cross state lines to obtain opioids. A national registry would prevent abuse through taking advantage of a localized system.

Additional Comments

We believe that the "knowledge" provision of section 171.103 (c) must be expanded to include circumstances where providers should reasonably know that their actions constitute health information blocking. This addition is vital to reinforcing the importance of health systems and providers prioritizing patient choice and the secure, safe transmission of information as guiding organizational principals.

Conclusion

OCHIN appreciates the ONC's efforts to modernize interoperability and address information blocking. We hope that our comments provide insight into the challenges we see with the current regulatory framework. We appreciate your consideration of our comments and we look forward to assisting the ONC in advancing interoperability.

Please contact Jennifer Stoll at stollj@ochin.org should you have any questions.

Sincerely,

Jennifer Stoll
EVP, Government Relations and Public Affairs