CENTER *for* MEDICAL
INTEROPERABILITY

May 31, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator
US Department of Health and Human Services
330 C Street SW
Floor 7
Washington, DC 20201

RE: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, RIN 0955-AA01

Submitted Electronically

Dear Doctor Rucker:

Thank you for the opportunity to respond to the 21st Century Cures Act: Information Blocking, and the ONC Health IT Certification Program proposed rule from the Office of the National Coordinator for Health Information Technology (ONC). The Center for Medical Interoperability (CMI) appreciates the administration's focus on achieving a more interoperable and patient-centered health care system. We look forward to working with ONC as it finalizes and operationalizes the policies included in this proposed rule.

The Center for Medical Interoperability (CMI) is a non-profit organization led by health systems with a mission to ***accelerate the seamless exchange of information to improve health care for all***. Modeled after centralized labs from other industries, CMI serves as a cooperative research and development lab as well as a test and certification resource to address technical challenges and ensure conformance to specifications that enable comprehensive interoperability, data liquidity, and trust. Initial draft specifications have been related to medical devices within the acute episode of care.[1] CMI's CEO-level board of directors identifies health care industry technology problems that, when solved, will benefit the public good and the health care industry.

[1] *Available at* https://medicalinteroperability.org/specifications/

CMI membership is limited to health systems, individuals, and self-insured corporations, but we work with a variety of stakeholders, including medical device manufacturers, electronic health record (EHR) vendors, standards development organizations, and others, to design and engineer the technical infrastructure that will enable comprehensive interoperability, data liquidity, and the trust needed to deliver person-centered medical care.

We believe that the delivery of health care in America can be vastly improved. In an increasingly digital age where data and technology have entered nearly every facet of our lives, the delivery of health care seems relatively unchanged. In most industries, technology and data have enabled better experiences, efficiencies, and outcomes. In health care, however, it seems that technology and data have increased both complexity and costs in an already confusing and expensive system. The Center for Medical Interoperability would like to change this. By collaboratively developing an industry platform that will establish a foundation of trust between technologies in health care settings from medical devices to electronic health records, CMI envisions a world where health care data is connected, digital, accessible, trusted, secure, and useful for providers and patients alike.

This proposed rule from ONC combined with the proposed rule from Centers for Medicare and Medicaid Services (CMS) on Interoperability and Patient Access (CMS-9115-P) are bold in both vision and scope. The future state envisioned by the policies set forth in these proposed rules puts the patient in the center of exchanging health care data. CMI supports the goals and underlying policy intention of both the 21st Century Cures law and these proposed rules. However, we also recognize the challenges that remain to achieve CMI's desired state of comprehensive interoperability, data liquidity, and trust. CMI stands willing to work with the Department of Health and Human Services (HHS) and others in federal and state government to drive toward a more functional and efficient health care delivery system on behalf of our members.

In the world envisioned by these proposed rules, a patient would request their data from a payer or a provider under their Health Insurance Portability and Accountability Act (HIPAA) right of access. The data would flow out of the payer or provider in a structured and usable format to the patient. The patient would collect their information on a personal electronic device by using third-party applications. The patient could then present their personal electronic device to a care provider to share their health information or the patient could electronically push the data onto the provider's health record system for use in treatment. ***This future state presupposes the existence of trust at every level of these interactions, but this trust does not yet exist.***

The federal government has taken an active role in digitizing the American health care system through incentive payments and adjustments through programs like Promoting Interoperability. But the lack of interoperability in health care will not be solved through government action alone. It is incumbent upon the health care industry to demand better care for our patients. Data should live in the hands of patients, be under their control, and flow to and from providers to inform better treatment and care for patients.

In order to achieve this, ***CMI is developing a platform to allow the trusted and secure connection of all technologies surrounding patient care.***

CMI believes that interoperability can be achieved by establishing an overarching technical architecture that supports the free flow of information on a vendor-neutral / non-proprietary platform. The technologies surrounding the delivery of health care will connect in a one-to-many, two-way, plug-and-play, standards-based and trusted manner. One-to-many means the ability to add a technology without jeopardizing others. Two-way means the ability to both send and receive data – leading to data liquidity. Plug-and-play refers to the ability to add, modify, or replace technologies without special effort on behalf of the user. Standards-based means adhering to established interface specifications. Lastly, everything on or in the platform will be trusted by conforming to technical requirements engineered to establish and maintain trust.

CMI is modeled on the belief that this platform must be driven by the purchasers and users of health technologies. ***Hospitals, health systems, and other large purchasers of health care technology and services, including HHS, should collectively align and demand that products adhere to the principles of platform architecture for data exchange.*** Benefits can be realized by all stakeholders. Right now, vendors often compete on the way that they present and process their information within their proprietary solutions. When technology vendors align on a common platform for interoperability, it will allow them to simplify and decouple their proprietary products by leveraging the data from not only their products but from any others as needed. The innovations, efficiencies, and improvements in safety that result will benefit everyone.

Ideal State

When a person enters the office of a care provider, they should be a known entity. The health care system should recognize the person, know their complete medical history, and trust the information shared by that person. Conversely, the person should know their care provider and trust not only the ability of the provider to deliver medical care but also that the information the patient shares will be used to benefit the patient, not misused, and not shared beyond that patient's wishes.

The patient's health history should be controlled by the patient and shared with the care provider prior to the patient's visit. If the provider needs additional information, the provider should be able to obtain it from other providers, payers, or other sources with the patient's consent.

During the patient's visit, any medical devices or equipment used should seamlessly share all data generated with any other equipment that needs it and the patient's record. That record should be controlled by the patient and shared with the provider. During the visit, the caregiver can access the patient's record and use the device data to inform the appropriate steps in care orchestration and delivery. Because the patient's record is complete, the caregiver can compare trends of measurements and lab results over time and across provider organizations to better inform the course of treatment. During the visit, the patient's record is continuously updated and accessible to both the patient and the caregiver.

Following the visit, the patient can share their health information and this encounter update with other caregivers to check their opinion or better inform other courses of treatment for other conditions. With the patient in control of their data, they can take better control of their health. The patient could also choose to share their information more broadly with other entities, like researchers. With more sharing under patient control and more rich data flowing from technologies like medical devices, more robust data will be available to help inform the future of health care and the development of new treatments and cures. New technologies and algorithms could be developed to leverage this rich data to improve the practice of medicine and potentially automate some processes.

Once the technologies surrounding the patient are trusted, connected, and the data flows seamlessly, true interoperability will open the doors of innovation in ways we cannot yet imagine.

Foundations for the Ideal State

Foundational to this ideal state of health data are three principles: comprehensive interoperability, data liquidity, and trust.

By "***comprehensive interoperability***," we mean that the technologies within an episode of care as well as across care settings and locations should be interoperable – from the medical devices used to monitor and provide therapy to patients, to the lab systems that test and diagnose, to the record system that stores and streamlines patient data for clinical use. True interoperability will come from communication across all technologies used in the delivery of health care. Typical discussions around health care interoperability center around the electronic health records systems, but these record systems are only one piece of the puzzle.

"***Data liquidity***" refers to the ability of the data to be accessed, exchanged, and used across platforms or systems without special effort or blocking from any direction. Information from one device must be useable by another to benefit the patient – otherwise the data lives in isolation and its utility is limited. Once data can flow across disparate technologies and be incorporated into each for use in the delivery of care, then the data has become truly liquid for the benefit of the patient.

"***Trust***," as we define it, is when the information and its source are recognized and credible. The data can be relied upon by a caregiver in his or her practice of medicine as clinically valid. We also mean that the data is traceable to its source, that its integrity has been maintained through transport and while at rest and this is verifiable by the end user, and that privacy is protected. Bidirectional trust is fundamental to health care – the patient must trust the provider and vice versa. When it comes to technologies, the recipient must trust the sender and vice versa. Without trust, these relationships cease.

Connecting Technologies through a Trust Platform

To enable comprehensive interoperability, data liquidity, and trust, CMI is working with its members, technology vendors, and others across the health care industry to design and develop a platform for trust in health care. The trust platform will allow data from different technologies to flow from devices, record systems, clinical databases, data registries, and tailored applications safely and securely across the entire health care delivery system. This platform is scalable from the individual episode of care to the operations of a large health system provider. At scale, this approach would unlock previously aspirational capabilities like predictive analytics, artificial intelligence, and other models that rely on identified, contextualized, and computable data to improve care orchestration. A trust platform will be able to leverage operations tools such as the automated and secure update of medical devices to protect against cyberthreats. At the very least, connecting health care technologies through a trust platform will allow providers to focus on treating patients and practicing medicine rather than entering data, troubleshooting technology, and juggling segregated data points vital to proper treatment.

Once developed, CMI will demonstrate the utility of the trust platform through specific use cases and provide implementation specifications and guidance to scale the platform across health care systems. Acting in our role as a centralized lab, we will test, verify, and certify products, tools, and solutions to ensure conformance to specifications enabling comprehensive interoperability and data liquidity and to help leverage the platform's architecture in new directions as determined by the health care marketplace.

Response to Proposed Rules

CMI is encouraged by the aggressive posture this administration is taking to liberate health data from proprietary systems and place it in the hands of patients. For too long, the health care system has been operating as a group of separate factions whose data has been locked in silos, limiting the data's utility for use in patient care or innovative applications and research. Providers have been required to purchase systems to comply with federal programs, but the systems have not worked as anticipated and require constant upgrades and maintenance at the expense of the purchasers. The 21st Century Cures law placed new requirements on technology developers to ensure the functionality of systems certified by the federal government and to increase information sharing between providers and systems alike. CMS's proposal goes beyond 21st Century Cures to require payers to share information in structured formats through easily accessible portals just as Cures required of developers and providers. Holding all participants in the health care industry accountable to the same sharing requirements will increase the flow of data and make it easier for patients and caregivers to access and use health information to improve outcomes.

CMI supports the adoption of common standards in Fast Health care Interoperability Resources (FHIR) and hopes that HHS will embrace the more advanced FHIR 4 standard in the final rule while simultaneously giving developers and systems adequate time to conform to the requirements. Balancing the timelines of the mandates in these proposals with the realistic burdens and costs faced by developers and providers will be key to the success of these proposals. Regarding information blocking, CMI is encouraged that these proposals will build toward a future where data is no longer held hostage. However, CMI is concerned that some of the definitions included are too broad to be reasonably enforced, and under CMI's view of comprehensive interoperability, it is unclear whether all technologies in health care, such as medical devices, would be covered by the information blocking provisions.

Finally, these proposals will do much to improve a patient's ability to access their own health information, but it is unclear how much these proposals will do to improve the flow of information internal to each episode of care, inside individual health care facilities, or between health care facilities and systems. Additionally, these rules do not address a crucial policy question around the privacy and control of digital health data that CMI believes is necessary before allowing sensitive health data to flow out of its traditional, protected pathways. As recent debates around consumer privacy increase and government struggles to determine the best path forward, separate industries in the private sector should come together to offer solutions to the broad questions of patient privacy.

CMI is developing a common platform to enable trust inside and outside of health systems and facilitate secure, omnidirectional exchange of all data types from any source that adheres to the specifications of the platform.

CMI believes that a trust platform approach is critical to both realizing the health care system of the future and resolving the questions around privacy because the platform design is agile and can adapt to support and implement policies determined by the marketplace.

Responses to Specific Proposals:

Updates to the 2015 Edition Certification Criteria

Adoption of United States Core Data for Interoperability (USCDI)

CMI supports the adoption of the United States Core Data for Interoperability (USCDI) Version 1 as proposed by the ONC rule. CMI is encouraged by the proposal of the Standards Advancement Process and urges ONC to allow developers, providers, and others to go beyond the baseline requirements of certified products. Because it is difficult for the federal regulatory cycle to keep pace with technological innovation in the private market, we counsel ONC to be flexible to allow for the use of new technologies, even those that may be disruptive to current practices as long as these technologies conform to acceptable standards of privacy, security, and data integrity and provenance.

Electronic Prescribing

CMI supports updating the SCRIPT standard for electronic prescribing to conform with updated rules from CMS. CMI encourages ONC and CMS to allow the private market to go above and beyond the functionalities of standards that may be required through various regulations. As long as providers and developers are meeting the baseline requirements set by CMS and ONC, they should be allowed to adopt more advanced standards that may allow for more innovative uses while still complying with the applicable requirements from ONC and CMS related to data integrity and provenance, privacy, and security.

Electronic Health Information Export

CMI is supportive in concept of the proposal to require "electronic health information export," but also recognizes the technical complexity faced by providers and the public policy challenges raised by creating a back door to protected patient data, particularly given the breadth of the definition of "electronic health information" (EHI) later in the rule. Data export will enable more free flow of information from developer systems and this outcome is necessary to achieve comprehensive interoperability and data liquidity. Without connection of a data export to a secure and trusted endpoint, however, the only achievement is removing data from a certified system. EHI export, as proposed, will allow patients and providers to access data from certified products, but they will not necessarily be able to use that data after export. For example, the lack of standardization around the EHI export requirement means the recipient will have to translate the export file into a useable format by the next system the file enters. As ONC points out, this portability of the export function will increase both a patient's ability to access their data and a provider's ability to transition between systems. ***However, without a trusted and interoperable mechanism of importation, the data may not be able to be received*** even with access to published export information as ONC proposes. The health facility importing the data would still need to expend resources to translate the data and verify its accuracy before it could be imported and used for patient care.

CMI urges ONC to listen to providers and developers regarding the technological burdens associated with EHI export functionalities along with balancing those needs with realistic expectations for their timelines.

Additionally, ONC specifically espouses a belief in this proposal that EHI export will "stimulate a vibrant, competitive market in which third-party software developers can specialize in processing the data exported from certified health IT products in support of patients and providers."[2] There likely will be greater exposure of patient health information to the patients themselves when developers design accessible and usable formats and interfaces for receiving and digesting health data. However, the breadth of health data envisioned as exportable under this proposed requirement, especially when married with the proposals surrounding information blocking, present a public policy problem that is enormous in scale: who should be granted access to a patient's identifiable health information and how can they use it? Some third-party developers

[2] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 7424, at 7448 (proposed March 4, 2019).

may be eager to begin mining health data and using it to improve their own data repositories to increase business opportunities. These proposals from ONC and CMS do not begin to consider these questions and ***CMI believes that advancing this type of export capability without considering these questions and related ramifications poses an enormous threat not only to patients, their privacy, and their trust in the health care system, but also the success of interoperability and these proposals at large.***

CMI believes it is incumbent upon the private sector to join forces between industries and provide a possible solution to these privacy questions. ***CMI will work with health systems to make the trust platform a mechanism to enable trust between health data technologies and third-party app developers who have not yet been subject to federal oversight regarding permitted uses and disclosures of patient data.*** The potential for misuse of patient data is tremendous and could impact patient lives directly regarding their employment, insurance policies, borrowing ability, housing, child custody, and more. This is why CMI takes seriously its role in promoting comprehensive interoperability and data liquidity by including trust as a foundational principle.

Federal encouragement of the free flow of health information necessitates the development of robust protections against the unauthorized use of such information. This includes the use of secure trust protocols and clearly defined allowable uses for every party involved in data use or exchange. Patients should have control, ability to monitor, assurances, and remedies in the case of breach.

Consent Management

CMI appreciates ONC's attention to this important issue. ***CMI believes that federal policies should advance toward placing the control of patient data, including consent, in the hands of patients themselves.*** By connecting all health technologies to a trust platform, the health care industry can get closer to comprehensive interoperability and data liquidity. Through a distributed, encrypted system of cataloging health information, including the metadata, exchange of health information could be in the patient's control without the need for a provider to be shouldered with the burden of unauthorized disclosures.

As ONC works toward a final rule, CMI encourages ONC to consider the possibilities of allowing for uniform and clear patient consent management and data controls through a trust platform. Additionally, CMI urges ONC to balance these consent proposals with other requirements for health privacy and the administration's recent considerations to update certain privacy regulations and policies. Providers and patients should be able to easily understand the rules of the road for sharing health information, and ONC can help foster this outcome by coordinating its efforts with those of others at HHS tasked with patient privacy, such as the Substance Abuse and Mental Health Services Administration and the Office for Civil Rights.

Health IT for the Care Continuum

CMI supports both the intent of the 21st Century Cures law in encouraging the certification of health technology products for different areas of provider need and the consideration of voluntary criteria to support pediatric treatment and care. CMI believes that connection of all health technologies and the use of their data can benefit all patients, including children, through improved outcomes. Generating more standardization across products used in pediatric care will advance providers' ability to continuously improve pediatric care. CMI encourages ONC to continue working with the provider community to advance this certification proposal and to work toward other areas where there is a need for more robust and certified health IT products.

Prevention, diagnosis, and treatment of opioid use disorder could also be greatly improved by the development, implementation, and widescale adoption of a trust platform across the health care industry. For example, aggregating data from patient monitors could give providers and researchers a better understanding of how patients respond to pain management in care settings and use of remote patient monitors could extend the reach outside the health delivery system. Once the data is liquid, algorithms can be introduced to automate alerts, orders for testing, or even a visit by a caregiver. Opioid use disorder is just one treatment area out of many that could be improved by connecting technologies through a trust platform.

Conditions and Maintenance of Certification

CMI is encouraged by new proposed requirements on developers to not block information, provide assurances to that end, and communicate openly with providers and other vendors as required by the Cures law. CMI believes it is vital that participants in the health delivery system adhere to common principles of communication and data sharing to improve patient care. As ONC works to finalize these proposals, CMI urges ONC to consider the potential burdens and costs that may be passed onto the purchasers of these products. Additionally, CMI urges ONC to listen to comments from developer and provider organizations regarding the proposed timelines for effective dates of requirements throughout the proposals for Conditions and Maintenance of Certification.

Application Programming Interfaces (APIs)

CMI urges ONC to adopt Option 4 or the FHIR Release 4 as the sole option for Certified Health IT. Our members have experienced significant effort navigating compatibility issues when moving from FHIR Release 2 to Release 3 and, consequentially, perceive general risk in migrating between FHIR versions. Additionally, FHIR Release 4 advanced several fundamental parts of the standard to a "normative" status, which assures future compatibility, and is the first release that lacks the "for trial use" brand over the entire release. We also ask ONC to work with providers who may struggle to adopt updated systems under the proposed timelines. ONC should take seriously comments from developers and providers regarding the burdens and expense of these adoption requirements and timelines, particularly the fees allowed of API Technology Suppliers.

Information Blocking

CMI appreciates the thought and detail given to the proposed rulemaking around information blocking and reasonable and necessary activities that do not constitute information blocking. Overall, ***CMI cautions against overly broad and vague definitions that may not withstand court challenges, potentially placing the entire prohibition on information blocking in question. Of vital importance to CMI's ideal state of interoperability is the explicit inclusion of all technologies surrounding the patient during treatment and care delivery.*** The term "observational health information" appears to get at this concept, but the definitions provided focus their attention on describing the actions of electronic health records and not medical devices or other modalities present in an operating room. Given that the ONC's authority is statutorily limited to the certification program and other activities surrounding electronic health records, it makes sense that the rulemaking would focus here. However, as the rules contemplate, the intention of Congress with discouraging information blocking relates to all health data that can be used in patient care. CMI hopes that HHS will find a balance of the authority given to the Office of the Inspector General (OIG) in Cures and other authorities in federal statute, such as those held by the Food and Drug Administration, to ensure both that information blocking is enforced broadly and that the regulations provide sufficient clarity and justification to withstand legal challenge. CMI believes ending the practice of information blocking is vitally important to achieving true interoperability.

Health Care Providers

As the Department considers the implementation and enforcement of information blocking, CMI encourages uniformity with existing laws and requirements placed on providers. Additionally, while information blocking should be discouraged across the health care system, the Department should balance the ramifications of potential enforcement and the need to exchange data to improve care with the realistic burdens and technical hurdles faced by the provider community. HHS should work with provider groups to ensure understanding of and prevention of information blocking. Because the Department is also considering changes to HIPAA, CMI encourages coordination across agencies and offices at HHS to simplify the requirements placed on providers. The rules of the road for data sharing should be clearly defined across the health care continuum, and they should be well understood by the provider community.

Health IT Developers of Certified Health IT

CMI believes that information blocking can occur outside of developers of certified health information technology, such as through medical devices or their interfacing software products. Because medical device data is vital to appropriate care delivery, CMI urges HHS to consider how information blocking of medical device data could be prevented under current authorities.

Networks and Exchanges

The proposed interpretation of "health information network" is very broad and more than envisioned in the 21st Century Cures law. Under the proposed definition of "health information network," any two systems connected to the internet could be considered a network and liable for potential information blocking claims if any of the information crossing the systems contained any of the information captured by the broad definition of "electronic health information." The intention of Congress was to hold accountable those who control patient health information and withhold it from use in patient care, delivery, or access to that patient or their care provider. To that end, "exchange" and "network" are nearly interchangeable. While ONC is correct that the Cures law does not define exchange or network, the Public Health Services Act uses both terms in many instances, and the ONC should use existing statutory interpretation and use as a guide to the same terms inserted in different instances by the Cures law.

For example in Section 3022(b)(C) of the Public Health Service Act as amended by the Cures law, the statute refers to a "health information exchange or network" when granting investigative and enforcement authority to the HHS Office of the Inspector General (OIG) suggesting their similar natures and the desire for their similar treatment under the law. Congressional intent was to bring other actors engaged in the exchange and control of health information under federal scrutiny beyond the provider community. With incentive payments to digitize health information nationally and encourage more use and exchange of health data, the federal government generated a large business economy for health information technology. However, the developers and middlemen in this economy were not subject to federal scrutiny for their behavior. Instead, the providers were subject to financial penalty for the failures of the developers' products or the middlemen to provide connections. ***Information blocking as described in Section 3022 was intended by Congress to bring these non-providers under the microscope of federal scrutiny to change behavior and encourage the flow of health information to improve patient care.***

Electronic Health Information

Congress intended that "electronic health information" be tied to the existing statutory definition of "health information" in the Social Security Act and used in the context of existing regulations. [3] Because "protected health information" as defined in regulation already encapsulates the statutory definition of "health information" that is transmitted or maintained in electronic media, CMI believes this term is best suited for use by HHS with regards to information blocking.[4] HHS should make this new legal construct of information blocking align with existing requirements to decrease confusion and administrative burden and increase the capability of those impacted to understand the policies and implications.

CMI urges HHS to ensure that information blocking includes all data generated by technologies surrounding patient care, but CMI believes that protected health information already includes these technologies. ***In order to advance to an ideal state of interoperability, all technologies that generate data about or for***

[3] 42 U.S.C. 1320(d)(4).

[4] 45 C.F.R. 160.103.

use in care of a patient must be held to the same standard of information sharing.

Price Information

CMI is supportive of HHS's efforts to make health care more transparent for patients, including pricing information. However, CMI urges a balance in these efforts and the efforts to make health care data interoperable for patient care and encourages the separation of price transparency policies from interoperability policies at this time. Because certified health IT products currently struggle to perform their intended function, CMI does not believe that HHS should consider requiring developers of certified health IT products to include a mechanism for patients to see price information since it is outside the scope of the clinical documentation information certified products are designed to handle. To the extent that HHS pursues the transparency of pricing and billing information through current authorities, it should focus the collection of this data on systems that more traditionally handle pricing and billing information, such as claims processing, revenue cycle management, and insurance data.

Access, Exchange, and Use

CMI is supportive of a broad interpretation of the terms "access, exchange, and use" as employed by the 21st Century Cures law and feels broad interpretation will support the advancement to true interoperability as described in our ideal state above. However, CMI urges caution as well when it comes to stretching HHS authority and regulatory reach. Ending information blocking is too important to the advancement of health data interoperability to be threatened with constant litigation related to vagueness, overreach, overbreadth, or other legal doctrines related to denotation and connotation of statutory text and its implementing regulations. CMI believes close counsel with HHS Office of General Counsel and the OIG will help ensure that enforcement actions against information blocking withstand legal challenge.

Interoperability Elements

CMI is supportive of the concept of "interoperability elements" as delineating actors in control over the actual access, exchange, and use of health data from those subject to that control. CMI urges HHS to examine the control of such elements while investigating claims of information blocking. Members of CMI have frequently raised frustrations regarding their ability to gain information from systems they have purchased and use daily in their facilities despite the sophistication and perceived power and influence of the member organizations. CMI particularly appreciates the discussion of providers being "locked in" to specific technologies when developers exercise control over the technology's ability to be functionally interoperable. To the extent that HHS considers health care providers as having the functional "equivalent to the control exercised by a dominant health IT developer, HIN, or HIE" because the provider has policies that govern information sharing over large areas, CMI urges HHS to consider the provider's policy versus the technology's functionality when determining the source of the information blocking.[5]

Observational Health Information

CMI believes that data generated by a patient or a technology connected to a patient should be able to be used by caregivers in patient treatment and care delivery. ONC's description of observational health information does not explicitly state that health information produced by medical devices during the course of patient treatment is observational health information, but CMI believes that ONC should state this directly. Medical devices surround patients during visits with care providers, but too often these devices do not connect or feed information to other technologies or systems. In order to achieve comprehensive interoperability, all technologies used in patient care should be held to the same standards of information sharing to make available the most information possible for patients and caregivers to improve outcomes. Observational health information generated by medical devices should flow through records systems and other technologies the same as every other data generated during the course of patient care.

Non-Standard Implementation Practices

Recognizing the need for standardized implementations, structures, and pathways for data, CMI urges HHS not to discourage innovative or disruptive technologies by enforcing conformance to specifications that may not allow for groundbreaking technologies to improve the flow and use of data for patient care.

Exceptions to Information Blocking

As raised by HHS regarding the Trusted Exchange Network, CMI believes that once the trust platform has been developed, implemented, and scaled, implementation of the trust platform by a health provider system could be considered a de facto exception to information blocking. As the trust platform is developed and implemented, CMI looks forward to working with ONC and others at HHS to explore this possibility.

- *Preventing Harm*

CMI encourages HHS to consider the extent to which patient harm may occur due to the information withheld that is the basis for a particular claim of information blocking.

- *Promoting Privacy*

CMI recognizes the importance of patient privacy and its role in establishing trust between providers and patients. Given the complexities of federal and state laws around privacy, consent, and the permitted uses and disclosures of patient health information, CMI urges HHS to work with providers, developers, and others to clarify the rules of the

[5] 84 Fed. Reg. at 7518.

road regarding information sharing and information blocking. The current requirements of HIPAA alone evade most people interacting with the health care delivery system. As HHS considers changes to federal privacy rules, such as the recent request for information on HIPAA, CMI urges HHS to adopt a consistent policy across regulatory regimes to facilitate understanding in provider, developer, and patient populations.

Given the privacy questions raised by the API and data export provisions of these proposed rules when combined with the current HIPAA right of access and the lack of regulation or even transparency in practices of the non-health care developer marketplace, CMI hopes that HHS will carefully consider this exception and the need for it to succeed. ***Without the ability to ensure privacy, trust cannot be established, and without trust, these proposals fall apart.***

Regarding the sub-exception proposed for "non-covered actors" that develop patient-facing health IT, CMI urges HHS to balance the requirements of this potential sub-exception with the requirements placed on covered actors who institute organizational privacy policies.

CMI also encourages HHS to consider the potential utility an industry-wide trust platform could provide in managing consent and privacy practices, especially when control of the data is placed in the hands of patients.

- *Promoting Security*

CMI encourages HHS to recognize that certain security breaches in health technology are unpredictable and can take time to diagnose and correct. HHS should work with providers to ensure that measures taken to respond to security threats are not claimed as information blocking to avoid unnecessary investigation for all parties involved. CMI also believes that connection through a trust platform can allow for more robust and agreed upon security protocols between technologies and avoid potential information blocking claims related to the security of health data.

- *Recovering Cost Reasonably Incurred*

Given the lack of true interoperability and a scaled trust platform across health systems, CMI asks HHS to consider the limitations currently in place related to information systems in use by its hospital members. Limitations placed on the ability of health systems to recover costs related to the implementation of these proposed rules and the systems upgrades they will require only increase burdens on health systems and providers. Administrative costs due to regulatory burdens have been a focus of congress and this administration in recent months, and this exception appears to limit the ability of health systems to use this exception to recover costs the same way it would allow a developer to recover costs. CMI urges parity in treatment of different actors who may qualify for this exception.

- *Infeasible Requests*

CMI will continue to develop an implementable trust platform to allow the connection of all technologies surrounding the patient in the delivery of health care. Once this platform is operational, CMI hopes this exception will no longer be necessary.

- *Reasonable and Non-discriminatory Licensing*

As with the exception regarding infeasible requests above, CMI hopes that implementation and adoption of a trust platform at scale will allow technology providers to connect their proprietary intellectual property to the platform to share information without the need to share the actual intellectual property.

- *Request for Information on Additional Exceptions*

As stated above, CMI would like to propose the concept of participation in the scaled trust platform as a de facto exception to information blocking. As the platform is developed, implemented, adopted, and scaled, CMI hopes to work with HHS on this possibility.

Registries Request for Information

In order to achieve bidirectional exchange with registries in all their forms, CMI believes an implemented and scaled trust platform would provide a novel approach for connecting registries to other technologies engaged in the platform.

Patient Matching Request for Information

CMI believes that the use of unique patient identifiers that can be leveraged by patients and participating private health care providers can enable timely and accurate sharing of data, easier consent management, and the creation of personalized care strategies based on complete data sets. One such solution has been successfully deployed nationwide in Estonia where a person, post-authentication, can easily access and share their health care records. Since the United States' health care system is fundamentally different in so many respects, scaling such a solution to our country remains a significant challenge. ***However, investment in and industry adoption of a trust platform, supported by an appropriate governance model, based on a distributed architecture with strong identity protocols could pave the way for a simplified patient identifier for use in health care delivery.*** This trust platform can leverage a competitive marketplace for secure identity solutions from commercial third-party enterprises.

While CMI believes that a secure identity solution will be superior to matching, we support HHS's efforts to improve patient matching in the interim. Focusing on data quality at the point of collection and alignment around common data elements for demographics would be helpful.

CMI believes the private industry can and should step forward to provide a standardized and secure patient identity solution to avoid the technical and operational challenges of matching. CMI is exploring key principles and the necessary technical features for a scalable architecture through a proof-of-concept implementation under development in our lab. We would welcome an opportunity to demonstrate this proof-of-concept to HHS and others once it is ready for presentation.

Thank you for the opportunity to submit comments on these proposals. We welcome the opportunity to work with you and other stakeholders on these topics.

Sincerely,

Center for Medical Interoperability

F.E. Cantwell

Ed Cantwell, President and CEO
8 City Blvd., Ste. 203
Nashville, TN 37209
info@center4mi.org
(615) 257-6400