CENTER *for* MEDICAL
INTEROPERABILITY

May 31, 2019

The Honorable Seema Verma, MPH
Administrator
Centers for Medicare and Medicaid Services
Attention: CMS-9115-P
7500 Security Boulevard
Baltimore, MD 21244

RE: Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Manages Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers, CMS-9115-P, RIN 0938-AT79

Submitted Electronically

Dear Administrator Verma:

Thank you for the opportunity to respond to the Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanged and Health Care Providers proposed rule from the Centers for Medicare and Medicaid Services (CMS). 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 CMS 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. 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 CMS combined with the proposed rule from the Office of the National Coordinator for Health Information Technology (ONC) on Interoperability, Information Blocking, and the ONC Health IT Certification Program (RIN 0955-AA01) 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.***

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

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 CMS, 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 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. 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.

CMI is encouraged that prohibiting information blocking 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:

Technical Standards

CMI supports the proposal to require Medicare Advantage organizations, Medicaid state agencies, Medicaid managed care plans, children's health insurance program (CHIP) agencies, CHIP managed care entities, and qualified health plans in federally-facilitated exchanges to adopt and implement open application programming interfaces (APIs). CMI believes this initiative will allow more access to patient data, and CMI also supports aligning these requirements with the standards proposed for implementation by ONC for certified health IT products in the ONC proposed rule. CMI is also hopeful that this proposal will have CMS's desired outcome of raising "consumers' expectations and

encourage other payers in the market to take similar steps to advance patient access and empowerment."[2]

CMI urges CMS to work with state agencies and plans regarding the effective timelines for these proposals as there is significant work to be done, and it is unlikely that states or plans will be ready by the proposed deadline next January.

CMI appreciates CMS's discussion of patient privacy and the differentiations between when developers would be covered under HIPAA and when they would be subject to scrutiny by the Federal Trade Commission (FTC).[3] It is particularly important for providers and developers to understand the rules of the road, and CMI encourages CMS and other offices and agencies at HHS to continue working to make privacy and data sharing rules, regulations, and their enforcement mechanisms more accessible and understandable. CMI believes that it will be vitally important for patients to "have the opportunity to become more informed about how to protect their PHI."[4]

However, as stated above, ***CMI believes that a thorough policy discussion is necessary regarding the patient privacy implications raised by this proposed rule, in conjunction with the ONC proposed rule, and how these could impact patient trust of the health care delivery system.*** Throughout CMS's proposed rule, the agency makes references to third-party app developers and the ability of patients to make better use of their health information by using these applications. It is true that there is great potential for innovation in the private sector, especially when data is unencumbered by restrictive privacy laws like HIPAA, the Common Rule, and 42 CFR Part 2. ***However, there is also great risk to patients when sensitive health information is disclosed to entities not subject to restrictions on the control and use of that information.*** Restrictions in current federal health data privacy rules place limits on how entities can use patient information and with whom they can share it to protect patients from potential discrimination in areas like employment, borrowing and lending, life insurance, and others. Many organizations that develop software and applications like those envisioned by HHS are currently under scrutiny for being poor stewards of consumer data – to give these same entities access to health data while these debates are ongoing seems premature and dangerous.

CMI is not a patient privacy organization, but CMI does represent its provider health system members as they strive to generate interoperability through their collective power in the private market. Trust is key to the success of this endeavor. ***Trust is foundational not only to every health care relationship, but also to the future of interoperability.*** CMI also views the patient as integral to the care

---

[2] Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanged and Health Care Providers, 84 Fed Reg 7610, at 7619 (proposed March 4, 2019).
[3] *Id*. at 7621 and 7622.
[4] *Id*. at 7622.

relationship and recognizes the need of the care delivery system to have the patient's trust. Many of CMIs members are working right now to inform their patients of the potential risks of allowing unregulated applications to use and disclose their personal health data. Providing information like this to patients is necessary not only to inform them of the potential risks, but also to clarify that the health system cannot be held responsible for the actions of these third-party app developers, legally or ethically. CMS and the Office for Civil Rights have been helpful in clarifying where the liability of a health provider ends with regards to HIPAA. Understanding this is important not just to the provider and health care community, but also to patients. Neither developers nor health systems can risk losing the trust of patients if they are to succeed as businesses or to improve patient care and outcomes.

The patient right of access is intended to give patients their health information for their own personal use, and patients certainly have the right to disclose that information as they see fit. Many developers will be able to improve the accessibility and usability of health information for patients, but others may "deploy direct-to-consumer applications specifically in order to profit from obtaining, using, or disclosing individuals' PHI (and potentially other information) in ways the individual either did not authorize or to which the individual would not knowingly consent."[5] CMI fears that CMS's suggestion that a patient could simply "lodge a complaint" if they are unhappy after their health information has been disclosed falls short of reasonable precaution concerning protected health information.[6] Additionally, the nature of data and disclosures is that there is no way of reversing the disclosure. As consumers have become more aware of how software developers are using their information, more public scrutiny and even outrage has started to permeate. Congressional committees are currently discussing how to respond to these consumer privacy concerns and news outlets such as *The New York Times* have dedicated projects to privacy as a national issue. A recent study in the *Journal of the American Medical Association* found that nearly every application for depression or smoking cessation shared data with third party services provided by Facebook or Google, but only a few of them correctly disclosed this fact in their privacy policies.[7]

CMI believes it is incumbent upon the private sector to get ahead of this conundrum by developing and deploying a trust platform architecture and governance structure on behalf of its health system members. CMI also believes it is in the best interests of app developers to actively engage in this discussion at the outset. If appropriate consideration is taken to generate a solution that fosters both data exchange and trust simultaneously, both the developer economy and traditional health care economy win, not to mention patients. CMI stands ready to work

---

[5] *Id.*
[6] *Id.*
[7] Kit Huckvale, John Torous, Mark Larsen, Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation, *JAMA Netw Open* (April 19, 2019), *available at* *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=twitter&utm_campaign=content-shareicons&utm_content=article_engagement&utm_medium=social&utm_term=042219*.

with its members and others inside and outside of health care to advance interoperability, patient access, and trust among all parties and associated technologies.

Patient Access Through APIs

As discussed, CMI supports patient access through open APIs and recognizes the importance of structuring data and interfaces to improve data usage and advance toward comprehensive interoperability and data liquidity. In addition to the patient privacy and trust issues discussed above, ***CMI believes it is vitally important for CMS and other offices and agencies to address how data returns to the health system in addition to getting the data out of health systems.*** In order to facilitate the two-way exchange of health information more than just an exit is needed, a trusted entrance for the data to systems is also necessary. Focusing on getting the data out of the system but not back in only focuses on part of the problem. CMI believes that the trust platform approach is the answer to both transmitting the data out of APIs but also enabling the importation of data back into health systems. Without trusted data re-entry, caregivers cannot use external information in clinical care because they cannot trust or vet its accuracy, integrity, or validity.

It is good that CMS is focused on the ability of developers to be able to "readily consume the data to support consumer-friendly display and other functionalities."[8] But CMI believes there also needs to be a focus on ensuring that data can also be readily consumed and used by providers in the delivery of care to patients. ***A trust platform will enable this two-way flow of data to drive these proposals toward comprehensive interoperability and data liquidity.***

API Access to Published Provider Directory Data

CMI supports making more information regarding plans transparent and available for patients to use in their decision making. CMI urges CMS to work with payers with respect to the technical requirements of this proposal and the timeline for effectiveness, and CMI appreciates the solicitation for comment and CMS' intention to incorporate feedback from industry.

Health Information Exchange and Care Coordination Across Payers: Establishing a Coordination of Care Transaction to Communicate Between Plans

CMI supports making health plans develop a process to facilitate the coordination of care and transitions between plans for patients. More transparency and data availability will increase patients' ability to coordinate their own health care. CMI urges CMS to work with payers with respect to the technical requirements of this proposal and proposed effective date of next January to ensure the success of this proposal and its intentions.

Care Coordination Through Trusted Exchange Networks

[8] 84 Fed Reg at 7627.

CMI supports the principle of connecting patients, providers, and payers through trusted networks for the exchange of health information as proposed by CMS, but CMI does not believe these networks will exist for payers to comply with CMS's proposed effective date of next January. CMI urges CMS to work with the private sector on a more achievable timeline so that all parties involved can benefit from the data exchange made possible by such national connectivity. ***CMI's trust platform approach has the same goal as this proposal by CMS, and CMI looks forward to working with CMS and other offices and agencies within HHS to achieve such connections and exchange.***

CMI also believes that there are other rich sources of data, such as medical devices, that will be key to providing information to improve patient care and outcomes. In addition to connecting medical devices and all other technologies surrounding the patient, adding payer information will provide a more complete picture of a patient's care experience and allow for more data to be operationalized through a trust platform architecture. The most important piece of these connections is that the data coming from one system can be used by another – the onramp is just as important as the offramp. By ensuring all sources are trusted and connected by common interfaces with standard rules and governance, the data can leave one system and enter another to be contextualized and used by a caregiver on the receiving end. Trust is necessary for this data to be used in clinical care and in analysis to inform future care.

Revisions to the Conditions of Participation for Hospitals and Critical Access Hospitals

CMI urges CMS to strongly consider comments by provider organizations and associations regarding this proposal. CMI believes that interoperability is vital to the future of health care delivery and the health care industry at large, but we also recognize the need to balance incentives and disincentives, especially when it comes to measures that could be catastrophic for some providers and communities such as those in rural areas.

Request for Information on Advancing Interoperability Across the Care Continuum

CMI believes that wide-scale implementation and adoption of a trust platform to facilitate comprehensive interoperability and data liquidity will allow for more practice areas to utilize technology to improve care delivery. Because Meaningful Use did not include many provider categories, many in the health care industry have struggled to afford expensive record systems. Expansion of government incentive payments in these practice areas would help drive more adoption. Additionally, the availability of a trust platform will level the playing field for adopting and implementing new technologies across care settings.

Advancing Interoperability in Innovative Models

CMI believes there is a tremendous amount of value in connecting all the technologies surrounding health care delivery through a trusted platform. Once the information is trusted and flows through a platform, it can connect to any number of functionalities or algorithms for the purposes of improving efficiencies and patient outcomes.

Interoperability will generate savings to the entire health system, including Medicare and Medicaid. According to a 2013 study released by the West Health Institute, interoperability of medical devices alone could yield $30 billion in annual savings – and that's only a fraction of all technologies.[9] The potential savings from electronic health records has also been well documented, but most studies assume that the records systems will be actually useful to caregivers instead of a burden or simply an additional step in a long checklist of regulatory requirements. Once records systems and medical devices both are connected to a common platform, data can be leveraged for action on all fronts.

CMI would like to work with CMMI on how a trust platform could help inform CMMI's work in specific areas of clinical practice and across all operations in the health care delivery system. Once scaled, use of a trust platform and the data collected and translated from it could be used to allocate resources more effectively and pinpoint inefficiencies in both health care delivery and related government programs. Once mature, the trust platform could serve as the backbone for all innovation models to help model participants share data and maximize their resources to achieve CMMI's goals of improving care, lowering costs, and aligning payment systems to support patient-centered practices.

RFI for Information on Policies to Improve Patient Matching

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

[9] The Value of Medical Device Interoperability: Improving patient care with more than $30 billion in annual health care savings, The West Health Institute (March 2013), a*vailable at* https://www.westhealth.org/wp-content/uploads/2015/02/The-Value-of-Medical-Device-Interoperability.pdf.

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.

Sincerely,

Center for Medical Interoperability

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