CENTER *for* MEDICAL
INTEROPERABILITY

February 12, 2019

Mr. Roger Severino
Office for Civil Rights
Department of Health and Human Services
200 Independence Avenue SW
Room 509F, HHH Building
Washington, DC 20201

**RE: Request for Information on Modifying HIPAA Rules to Improve Coordinated Care, HHS-OCR-0945-AA00, RIN 0945-AA00**

Dear Mr. Severino:

Thank you for the opportunity to comment on how Health Insurance Portability and Accountability Act (HIPAA) regulations should be modified to promote care coordination and the transformation to value-based care while preserving the privacy and security of protected health information (PHI). We applaud the Office for Civil Rights (OCR) and the Department of Health and Human Services (HHS) for recognizing the need to improve existing regulations to keep up with the evolving technological ecosystem and to support the ultimate aims of a truly person-centric health care delivery system.

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 healthcare 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 related to comprehensive interoperability, data liquidity, and trust. CMI's CEO-level board of directors identify healthcare industry technology problems that, when solved, will benefit the public good and the healthcare 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.

A sound, long-term strategy for governing the use of digital health information and PHI is necessary to achieve the goal of improved care at lower costs while protecting individual privacy and security. In order for these transformative changes to proceed in

alignment with the goals of patients, data stewardship, ownership, permission, and control must be considered and incorporated into current and future privacy and security regulations. The HIPAA Privacy Rule and other regulations should be modified to address challenges and facilitate opportunities in an evolving digital ecosystem. The modification of these regulations should proceed in a way that protects and prioritizes the interests of individuals – and the health systems and clinicians who care for them – while allowing the marketplace to innovate and interact with individuals and their PHI in a responsible and controlled way.

While CMI supports modifying HIPAA to promote effective care coordination and reduce administrative burden, we encourage OCR and HHS to think beyond initiatives that produce incremental improvement in favor of supporting the creation of an expanded national trust and security platform that addresses not only privacy and security but also important topics such as patient identity and interoperability — a current focus for the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC).

Trust is not only key to achieving the aims of HIPAA, it is critical to the success of all healthcare interoperability and security related regulations and initiatives, like Promoting Interoperability, the proposed rules for information blocking and interoperability and patient access, the Trusted Exchange Framework and Common Agreement, and others. Without trust, a national patient matching and identification initiative will fail. Without trust, provider organizations and patients will not feel safe or comfortable with the external marketplace consuming PHI into applications through an open application programming interface (API). Without trust, healthcare provider organizations will be forced to rely upon only their own internally-curated data instead of working in concert with others. Without trust, medical errors persist and costs rise.

To provide trust, investment in and industry adoption of a trust platform technology architecture, supported by an appropriate governance model, is necessary. This platform will enable secure, comprehensive interoperability and data liquidity throughout the healthcare experience for individuals at the point of care, between care settings, and with the external marketplace. The CMI trust platform approach is based on a distributed, encrypted, ledger-based technology architecture with strong identity and security controls for data access, privacy, integrity, and provenance. This type of solution can connect any number of data sources, including medical devices, EHRs, organizations large and small, and most importantly people in an efficient and secure way allowing for the trusted exchange of information. This approach has many advantages over legacy and point solutions. In addition to being low maintenance and cost-effective, a distributed, encrypted, and ledger-based design is reliable, secure, private, and scalable. We can learn from examples where similar trust platforms have been deployed at scale with remarkable results. Estonia has used distributed, encrypted, and ledger-based technology on a national scale to allow individuals dynamic access to their own digital health data. The Estonia digital citizen approach is the global standard.

In practice, these concepts create an environment where all Americans will have a digital longitudinal record of their health and wellness. Because trust is built into the platform through the technology architecture and the associated governance model, the patient becomes a known entity with truly portable PHI recognizable by health systems

without concerns for patient matching and identification. A distributed, encrypted trust platform like this is flexible enough to scale across large systems and networks as well as down to the level of the patient within a specific episode of care, enabling an interoperable environment of devices and other modalities not yet seen in healthcare. This level of trust, security, and connectivity among technologies would improve patient safety and reduce caregiver burden. As a person moves in and out of healthcare settings, his or her data would be omnipresent but secure. The burgeoning marketplace of health applications will continue to flourish as long as it has open access to PHI, but the patient will lose unless all data users have met rigorous standards of trust.

We appreciate the opportunity to provide input during this critical step and urge OCR and HHS to incorporate the principles and recommendations discussed below when considering the future path of HIPAA and related regulations.

**Responses to Selected Questions**

*Questions 1 – 4*

Individuals should be able to access all of their PHI at all times. Access to PHI should be controlled and governed by the individual through use of a trusted and secure platform of electronic exchange. Understanding the limitations of the current system of records and release of information processes, OCR should strike a balance between the patient's right of access to their own PHI and the burdens on health systems to produce such information under any proposed timeline. However, CMI strongly encourages OCR to consider the potential for a trust platform to bring about comprehensive interoperability and data liquidity so that patient requests and their processing are immediate and automated. Now is the time to build upon the investment in EHRs and allow health systems, citizens, and the marketplace to add a trusted personal longitudinal health record.

*Question 5*

An individual should be able to access his or her PHI from any entity with the information through secure exchange over a trusted platform. However, protections against the unauthorized disclosure of PHI should follow any expansion of the ability to disclose such information.

Congress has clearly stated its intention to allow patients to access their information from businesses willing to provide it to them. Section 4006(b) of the 21st Century Cures Act clarified that "if the individual makes a request to a business associate for access to, or a copy of, protected health information about the individual, or if an individual makes a request to a business associate to grant such access to, or transmit such copy directly to, a person or entity designated by the individual, a business associate may provide the individual with such access or copy, which may be in an electronic form, or grant or transmit such access or copy to such person or entity designated by the individual."[1] Given the current inability of patients to track their health history to build their longitudinal health record, claims information presents a unique opportunity for

[1] 42 U.S.C 17935(e)(2) (2016).

patients to map their entire health history. CMI believes that unlocking data from more sources will allow patients to better access and use their health information to make more informed decisions and receive better care, but CMI cautions OCR that increasing disclosures without a trust platform could undermine patient privacy and the security of PHI.

*Questions 6 – 12*

Given the current structure of health information exchange, health care providers face delays and barriers when attempting to obtain PHI from other covered entities. The adoption and use of a trust platform can transform the mechanics of health information exchange and decrease these delays and barriers. HIPAA does not currently require covered entities to disclose PHI to other covered entities or non-covered entities, and the nature of the fee-for service payment system disincentivizes these disclosures.

As OCR considers requiring covered entities to disclose PHI when requested by other covered entities for treatment purposes, the treatment and care needs of the individual should be considered above all other concerns. OCR should, however, balance the potential burdens, including costs, placed upon providers to share information with other providers given the current lack of a trust platform.

Given that Congress discouraged information blocking in the 21st Century Cures Act, CMI believes that any changes to requirements for the disclosure of PHI should conform with the regulations related to information blocking.

*Questions 13 – 15*

Individuals should have visibility and control over the transmission of their own health information through a trust platform of distributed and encrypted information. Adoption of such a platform could provide the ability for individuals to be much more precise with the permissions and sharing of their health information. The trust platform model allows individuals to securely share only the PHI pertinent to a given interaction. As OCR considers allowing individuals to selectively segment their own health information for disclosure, it should weigh the needs and benefits of sharing complete and accurate information to provide the best possible care to patients and prevent misdiagnosis and death, including death from overdoses. A trust platform will be able to accommodate both the very limited sharing of information as well as the comprehensive sharing of information to conform to whatever the law, regulations, and preferences of the patients and care teams dictate. Any proposed changes to the segmentation of health information should comply with all other health privacy laws and regulations.

*Question 16*

OCR should ensure that any changes to HIPAA are consistent with rulemaking regarding interoperability and information blocking.

*Question 17*

The use of a trust platform that allows for patient-mediated exchange of distributed and encrypted health information will allow for more complete and timely disclosure of such data to improve treatment and care coordination. CMI believes that true person-centric data liquidity will enable a more efficient health system and result in better care for patients while also rendering the minimum necessary standard moot.

*Questions 18 – 20*

In a technical sense, one participating organization in a trust platform is no different from any other. A social services agency could be the recipient of data about a person in the exact same way as a healthcare provider organization. Consumer-mediated exchange of health information through a trust platform will establish direct sharing of information with these social services programs, community-based support programs, and other patient supports. CMI believes that cooperation and information sharing among various care providers results in the best patient outcomes. As OCR considers expanding HIPAA disclosures to other aspects of available health and social services, CMI urges the adoption of a trust platform to allow for seamless exchange of PHI through patient control.

*Questions 27 – 42*

The current structure of health exchange and antiquated information systems makes accounting for disclosures difficult and expensive. The use of a distributed, encrypted, ledger-based trust platform would simplify accounting for disclosures and allow patient access without burden or cost on the health system. In fact, the responsibility currently held by covered entities would be greatly alleviated. Individuals should have full visibility into their own data usage audit trail, including usage by covered entities, business associates, or any other entity that may be using their PHI. Also, the individual should have full visibility into the reason for the disclosure to covered entities, business associates, and other third parties.

As the volume of available digital health data and the potential applications for that data expand, so does the rapid growth of a new economy and marketplace of entities that have previously been outside of healthcare. While it may be tempting to allow access to PHI for any entity that claims to operate under the banner of "promoting care coordination," **OCR should take note of the broader current consumer privacy debate**. In this new health data ecosystem, the rules and processes that govern and protect PHI must be sensitive to the reality that not all covered entities, business associates, and third parties are created equal. It is important to vet not only the entity that will be using the PHI but also the end to which the PHI will be used. For instance, if a company is requesting PHI to fulfill a treatment purpose but is simultaneously mining, aggregating, and monetizing that data in another business line or product offering, this should be made known to the patient. The consent or authorization to use or disclose PHI should rest solely with the individual and be carefully regulated to avoid violations of personal privacy and security.

## Conclusion

The pace of technological change, agile market forces, and increasing use of data in healthcare necessitates a modern approach to the governance of health information. CMI realizes the need for modifications to HIPAA and its Privacy Rule. However, incremental changes that do not envision comprehensive interoperability, data liquidity and trust will not be sufficient to support a value-based and patient-centric health care delivery and payment system.

The current system for accessing and exchanging PHI in America is not capable of addressing the challenges and opportunities related to its protection and use. Without an emphasis on ubiquitous trust in healthcare, exploitation and misconduct are inevitable. Trust is the prerequisite for all digital health initiatives.

CMI proposes a coordinated effort to establish a pervasive trust platform that facilitates the secure transmission and use of PHI among not only covered entities and business associates but the entire marketplace. The CMI trust platform approach is agile enough to ensure robust, person-centered data privacy and security controls while allowing flexibility for long-term growth and innovation in the industry. CMI has begun this work in collaboration with its member organizations, which represent the largest healthcare systems in America, but it cannot succeed on its own. Meaningful progress will require bold and intentional action from government and healthcare leaders.

OCR, CMS, ONC, and other agencies at HHS have the ability to become change agents in this journey. The government is uniquely positioned to create and incent a technological trust platform that will help create a truly learning health system where patients, clinicians, and caregivers win. OCR and HHS should explore and embrace the CMI trust platform approach, and it should use its available levers to compel change and encourage rapid innovation across the industry and marketplace.

It is time to devote the nation's resources and attention to solving the issue that will make it possible to create the patient-centric health care system that we envision. The Center for Medical Interoperability urges OCR, CMS, ONC, and all of HHS to consider our recommendations. We stand ready to assist with HHS's initiatives.

Thank you for your consideration. We welcome the opportunity to work with you and other stakeholders.

Sincerely,

Center for Medical Interoperability

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