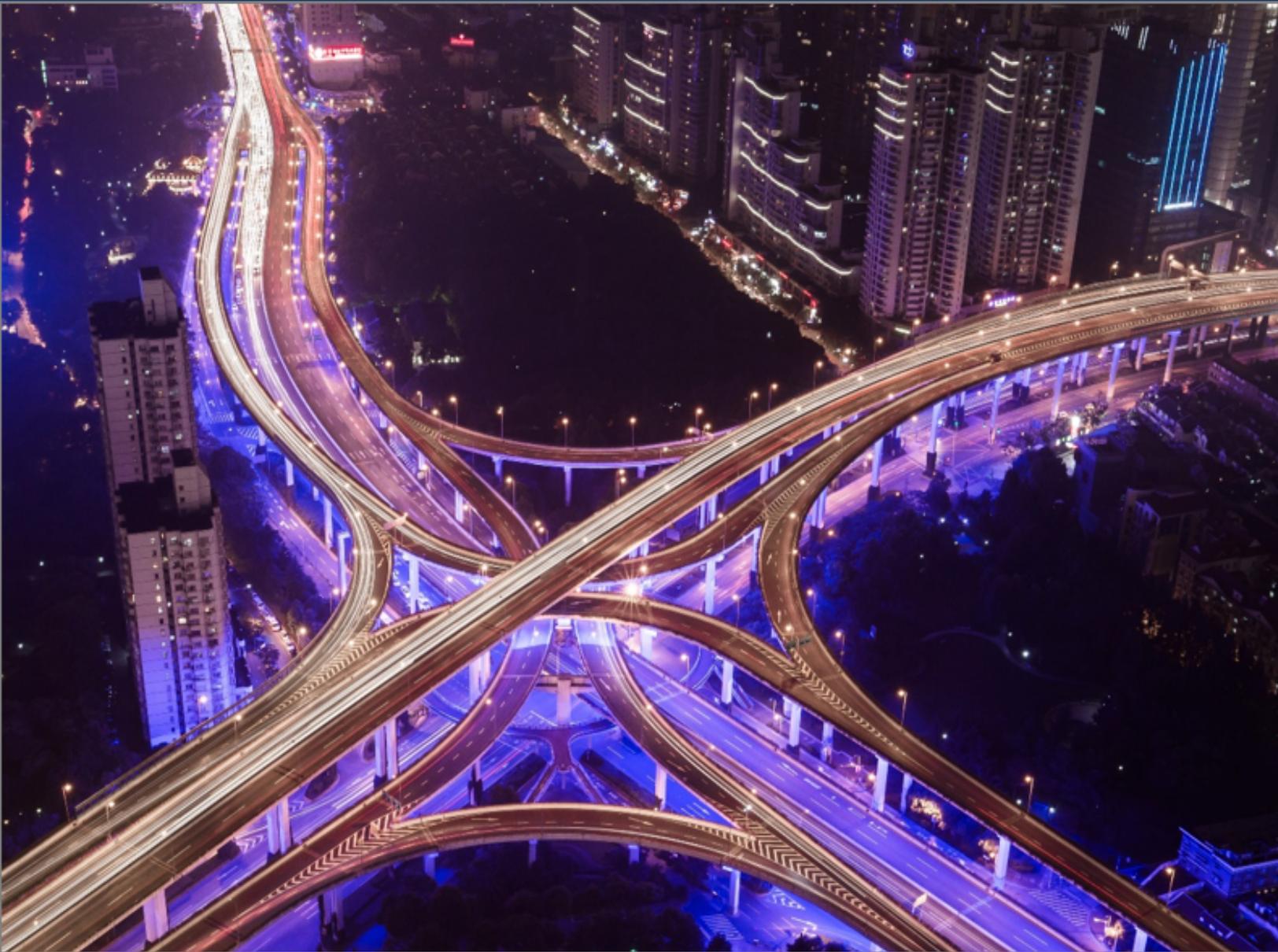


Healthcare Trust Platform

The key to meaningful industry transformation



Meredith Karney, Vice President, Health Economics and Value
Center for Medical Interoperability
January 2020
www.c4mi.org



© 2020 Center for Medical Interoperability. All rights reserved.

8 City Boulevard, Suite 203 Nashville, TN 37209

(615) 257-6417

www.c4mi.org

Trademarks

C4MI is a trademark of Center for Medical Interoperability. All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

This document is furnished on an "AS IS" basis and neither C4MI nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and C4MI and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by C4MI or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from C4MI, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Lifetime

C4MI reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein. Please refer to www.c4mi.org for the most current information.

Table of Contents

Introduction.....	4
Challenge	4
Ideal State.....	5
Foundations for the Ideal State	6
Solution	6
Summary	12
Learn More.....	13

Introduction

The U.S. healthcare delivery system is in need of major transformation. Numerous attempts have been made to reform the system but these have failed to control costs and address the major care quality variations that persist. A new approach that focuses on aligning the system and its supporting infrastructure around value for the patient is beginning to take hold.

Delivering high value care will require patients to have full access to their health information and to be able to share it across disparate technologies, systems, and providers. Access not only to data, but to usable insights, becomes essential if we hope to achieve the goals of the *Triple Aim* and the potential of personalized medicine. As promising as our future may seem, the transformation to value can either be stifled or promoted by the quality and usability of our supporting technologies.

Efforts over the last decade have made substantial headway to accelerate the implementation of information technology (IT) in health care. However, the capabilities of today's IT infrastructure still fall short of achieving a *learning health system*.¹ Given government's shifting approach toward "Promoting Interoperability" and the pressing need to accelerate the implementation of value-based care, this is a crucial time to rethink IT strategy for all stakeholders.

What the healthcare industry needs is a modern technology infrastructure and data sharing platform that enables digital health information to flow seamlessly, privately, and securely wherever it needs to go. The Center for Medical Interoperability ("C4MI") believes that this future state requires a new technology paradigm that connects all technologies across all healthcare settings with a secure platform. With this new **Healthcare Trust Platform**, we will finally be able to assemble a complete picture of a patient's health with data from medical devices, electronic health records, billing systems, and even mobile technologies. And we will be able to do it in a way that allows patients to be in control.

In this white paper, C4MI sets forth a strategy for developing and implementing the Healthcare Trust Platform to enable the trusted and secure connection of all technologies involved in patient care.

Challenge

While the HITECH Act catalyzed the move from paper to digital records via incentives and penalties for health care providers, it did not, unfortunately, address or create an underlying interoperability infrastructure to enable data liquidity among technologies. In the case of electronic health records (EHRs), it is the provider organizations that have been left to bridge

¹ *The Learning Health System and its Innovation Collaboratives*. Institute of Medicine. 2011.

the gap with everything from integration and interface engines to workarounds that lead to significant “clicks” for clinicians to even a combination of electronic and manual processes. What we have ended up with is a partially digitized system that still operates in proprietary data siloes and is actually more complex and burdensome than before.

The frustration with the current state of affairs has led the government to consider allowing third party applications and private market companies to solve the health industry’s problems. A 2019 CMS proposed rule states that they wish to “enable patients to access their health information electronically...to make the data available through an application programming interface [API] to which third party software applications connect to make the data available to patients.”² However, providing unvetted third party applications fairly open access to patient digital health data is problematic from a consumer privacy standpoint.

C4MI believes there is a way to do both--to simultaneously protect personal privacy of digital health care data while allowing the external marketplace of tech companies and innovators to interact with health care data in a responsible and productive way.

Ideal State

In an ideal world, a patient would enter the office of a care provider as a known entity. Their complete medical history should be accessible, and their provider should be able to clinically validate the digital information that the patient may share. The patient should, conversely, be able to trust that their care providers are using their personal health information in a responsible way.

The patient should have full control of their personal health record and should have the ability to share it with their care provider prior to a visit. If the provider needs additional information, they should be able to obtain it from other clinicians, payers, or other sources with the patient’s consent.

During the patient visit, any medical devices or equipment used should seamlessly share all data generated with any other equipment that need it as well as with the patient’s personal health record. That record should be controlled by the patient and shared with the provider. During the visit, the caregiver should be able to access the patient’s record and use analytics to analyze information to aid in care orchestration and delivery. Because the patient’s record is a single instance source of truth, the caregiver should be able to compare clinical and biometric trends over time and across organizations to better inform the course of treatment. The patient’s record should be continuously updated and accessible to both the patient and the care provider. Following the visit, the patient can automatically update their health

² 584 Fed. Reg. 7610, 7612 (Mar. 4, 2019).

information with other caregivers and researchers to check their opinion or better inform other courses of treatment for other conditions.

With data sharing under patient control and with access to richer data flowing from technologies, like medical and mobile devices, more robust data will be available to help inform the future of health care and the development of new treatments and cures.

Foundations for the Ideal State

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

Comprehensive interoperability means that 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 source 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, only then has it become truly liquid for the benefit of the patient.

Trust is achieved when the information and its source are recognized and credible. Data can be relied upon by a practitioner as clinically valid. Trust means that the data is protected and traceable to its source, that its integrity has been maintained through transport and is verifiable by the end user. 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.

Solution

Healthcare Trust Platform

To be able to operate and compete in the healthcare system of the future, the industry needs establish an overarching software architecture that supports the free flow of information on a vendor-neutral, non-proprietary platform. C4MI is working in coordination with its health system members, technology vendors, and others to develop the Healthcare Trust Platform

(“Trust Platform”), which supports comprehensive interoperability, data liquidity, and trust among digital health data. The Trust Platform is a wide-ranging solution that encompasses all health-related digital information on a single platform architecture with an accompanying policy and governance structure.

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 will unlock previously aspirational capabilities such as 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 operational 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.

The trust platform approach leverages a platform model to provide size, scale and trust characteristics to accelerate adoption without overhead. This is facilitated via an underlying technical architecture that creates uniform interfaces and data models for communication and an accompanying governance model to allow stakeholders to participate safely with conformant systems. This approach enables fast adoption at massive scale and at low cost. The Healthcare Trust Platform is comprehensive across healthcare settings in that it encompasses trusted data interoperability and interactions at the point of care, between care settings, between locations and organizations, with the person, and with the external application marketplace.

Once developed, C4MI 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 its role as a centralized lab, C4MI 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.

Trust Characteristics and Requirements

This section and the figure below present an overview of trust characteristics and requirements and how they are implemented within the Healthcare Trust Platform architecture.

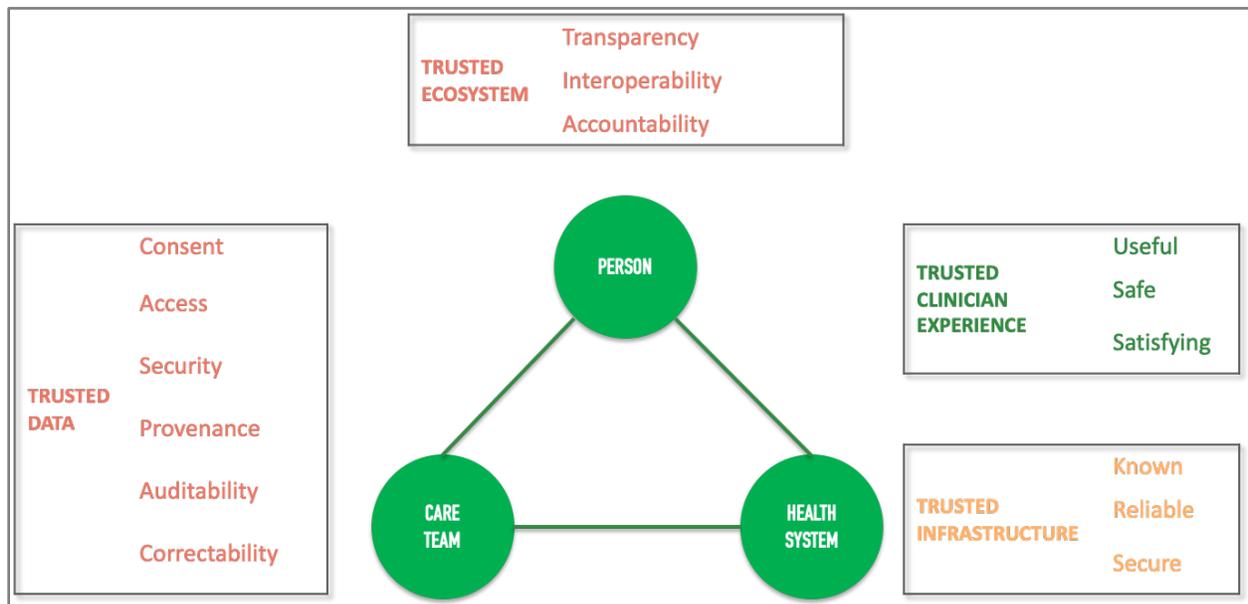
Transparency

Individuals should have access to and be able to control their digital health data -- where and how it is stored, how it is used and shared, consents they have provided, and how data is protected and retained. This is true of identifiable, pseudo-anonymized and deidentified data. Data can be generated at various points in time, for instance, patient data at episodes of care or prescriptions approved by clinicians. It may also be derived or transformed for various reasons for use in population health and personalized analytics.

The Healthcare Trust Platform provides mechanisms for collecting and conveying data transparency information and implements these by providing transparent data models and functions. The requirements around provenance also ensure that the data is tracked within the platform.

The governance model incorporates uniform data access and usage policies required for participating stakeholders to ensure transparency is maintained across all participants. Finally, the technical architecture, including functions, transactions, data models, security requirements, and services, are all made public.

Figure 1: Healthcare Trust Platform Characteristics and Requirements



Consent, Education, Use & Disclosure

Consent refers to a stakeholder's ability to know and control how their data is used, shared or disclosed, including who can access data and for what purpose, and the ability to revoke consent. A stakeholder may also desire to be educated on the implications of a positive or negative response to a consent request.

The trust platform requirements provide mechanisms for:

- Requesting and responding (e.g., accept, deny, request for more information) to consent
- Modifying and revoking consent
- Communicating consent
- Maintaining an audit trail of consent transactions
- Sharing consent status with data transactions (e.g., to make sure that recipients of data can be aware of the consent status)

The trust platform implements these requirements as a trust service through consent transactions, accompanying data models, and a cryptographically provable transaction log. The platform governance model ensures that stakeholders only use data as consented.

Access & Correctability

Access refers to a stakeholder's ability to view data about themselves from anybody who has it. Correctability is the capability of a stakeholder to request corrections against inaccurate data, including updates related to the 'right to be forgotten.'

The Trust platform technical requirements:

- Ensure data to stakeholder associations are maintained so that view requests can be supported
- Provide mechanisms for corrections to be reported and to convey the status of such requests.

The trust platform provides trust metadata to allow for data to stakeholder associations to be stored and transmitted along with the data and supports functions to retrieve requests to access and correct data from authorized entities. The governance model provides the supporting policies to ensure all participating stakeholders conform to these requirements.

Security

Security refers to various functions, such as:

- Protecting data from unauthorized access and changes, and recognizing if such changes occur
- Preventing unauthorized, unwanted and unintentional access to data (e.g., patient records) and interfaces; and, guaranteeing that data transactions occur only between intended recipients

The trust platform will support:

- Mechanisms to authenticate and authorize all stakeholder elements that store, transmit or receive data
- Ensure that all data transactions are protected from manipulation, eavesdropping etc.
- Provide mechanism to ensure privacy when required and keep track of transactions

The trust platform incorporates mechanisms for identity, authentication, authorization, integrity, encryption, and transaction logs.

Provenance

Provenance is a record of ownership of data and a chain of custody to trace the path of data transfers with or without modifications. When changes are made, it is also desirable to be able to recognize new updates and their author.

The trust platform provides ways for provenance information to be included whenever data is shared, including changes to related notes that may be useful. The technical architecture facilitates this capability via the provenance metadata model that is included as part of the trust metadata with any data transactions. The governance model ensures that the stakeholders populate this data in a conformant manner.

Accountability

International, federal and state laws may govern the responsibilities of health data stores, transmitters and consumers. In addition, business and legal agreements between stakeholders may impose additional requirements.

The governance model lays out uniform policies, procedures and agreements that ensure participating stakeholders conform to applicable legal and business obligations. The technical architecture provides ways to store information detailing data storage, transmission and usage in support of this requirement. This is facilitated via data and message integrity functions,

auditable transaction logs, and extensible data models that can support usage and consent constraints.

Interoperability

Interoperability refers to the ability of the stakeholders within the trust ecosystem to seamlessly exchange and make use of information. Interoperability enables data liquidity and an environment where data securely and seamlessly flows across and within stakeholder systems. This quick and on-demand trusted access to data, and associated information by care team members, patients, and other authorized recipients, enables better clinical outcomes, facilitates person-centered care, and reduces clinician burden.

This is a core requirement of the C4MI's mission and, hence, of the trust platform. C4MI's prior efforts have already laid the groundwork for an interoperable architecture among trusted ecosystem participants. The trust platform leverages this prior work and expands on it via additional uniform interfaces and data models that enable conformant architecture elements to connect and communicate in a plug-and-play, trusted, two-way, secure, standards-based manner. The governance model requires that stakeholder systems communicate using elements that conform to the trust platform architecture.

Auditability

Auditability is the ability to have visibility into data exchanges, including between health care organizations and consumer applications, over time. This is helpful for factors such as verification, timeline development, and non-repudiation.

The Trust Platform provides for all transactions to be logged in a manner that can be used for auditing and provide a mechanism for audits. The trust platform architecture accomplishes this by storing a log of all transactions on a cryptographically provable transaction log via a uniform set of interfaces. It also provides for an audit service to facilitate this. The governance model ensures that participating stakeholders meet the associated process requirements.

Trusted Infrastructure Characteristics

Infrastructure refers to the non-human systems that are used by stakeholders to communicate data. To ensure trust, all infrastructure elements need to be known; that is, they can be uniquely identified and authenticated prior to communications. They also need to meet reliability requirements that are identified by the governance model. Finally, both the elements and the communications need to be secure and to be able to support the trust data characteristic of security, while protecting them from being compromised.

C4MI's foundational efforts have taken initial steps to ensure trust within ecosystem participant internal architectures. The Trust Platform architecture leverages these efforts to achieve cross-stakeholder communications.

Clinician Trust Characteristics

For a clinician to trust technology, it must be useful, safe, and satisfying. While this can be subjective, the trust platform confers aforementioned characteristics to the ecosystem, removing barriers to creating solutions and spurring innovation.

Summary

The health care digital landscape continues to change rapidly. There is no question that the changes in health data interoperability, privacy and trust will continue to present risk and opportunity for many stakeholders. It is up to patients, providers and the health care industry to evolve and adapt in order to succeed in these opportunities of the future. Their success and survival depend upon having insight, agility and operational efficiency in their technological systems.

The Healthcare Trust Platform is an architecture for dynamically orchestrating secure data flows across components in and outside of a healthcare enterprise, including medical devices, electronic health records, clinical decision support systems, patient administration systems, and mobile technologies. This patent pending innovation enables plug-and-play interoperability via standards-based, trusted, bi-directional communication between components. Additionally, it allows for an efficient process to remotely manage medical devices via automated or semiautomated command and control processes.

The Healthcare Trust Platform will:

- Enable seamless exchange of data across the Trust Ecosystem, including the healthcare enterprise, care teams and people
- Enforce trusted data exchange in an open and vendor-neutral interoperable technology environment
- Economically scale across the healthcare industry

In order for the healthcare industry to sustain itself and maximize its outcomes, it needs viable solutions, like the Healthcare Trust Platform, that provide support for value-based care models, data analytics and precision medicine. C4MI provides the health care industry with flexible, modern technology to accelerate a meaningful transformation to improve health care for all.

Learn More

For the latest information about the Center for Medical Interoperability, please see the following resources:

- [C4MI Technical Documents and Specifications](#)
- [C4MI Public Policy Comments](#)

The author would like to thank Chris Riha and Brett Meeks for their contributions to this article's preparation.

Meredith Karney, Vice President of Health Economics and Value at the Center for Medical Interoperability, has spent her career testing and demonstrating the efficacy of new health care models that drive improved performance, sustainability, and quality. Her work aligns the business goals of providers, vendors and government so that interoperability is seen as a competitive advantage. Her primary research focuses on economic sustainability and the development of technical and administrative measures to enable effective care coordination in health care.