Silicon Flatirons
A Center for Law, Technology, and Entrepreneurship at the University of Colorado

*Roundtable Series on Entrepreneurship, Innovation, and Public Policy**

Policy Solutions to Fulfill the Promise of the Health Information Transformation

Chris Laughlin†

November 2015

Colorado Law
University of Colorado Boulder

*The Silicon Flatirons Roundtable Series on Entrepreneurship, Innovation, and Public Policy is sponsored by Brad Feld, Managing Director of the Foundry Group. This is the 41st Flatirons Report. More Reports - on topics including private equity, internet governance, cloud computing, angel investing, and modern pedagogy – can be found at http://www.siliconflatirons.com/publications.php?id=report. Roundtable and Summit discussions further the Silicon Flatiron Center's goal of elevating the debate around technology policy issues

† Chris Laughlin is a third year law student at the University of Colorado Law School.

Introduction

The healthcare system is transforming to a patient-centered model and opening up avenues of innovation. The availability and exchange of patient health information is integral to that transformation. The government is driving the transformation in part by opening up health data to providers[1] and requiring

[1] Kenneth Corbin, *Medicare data available to help businesses 'shake up' healthcare*, CIO (June 4, 2015, 5:47 AM), http://www.cio.com/article/2931480/healthcare/medicare-data-available-to-help-businesses-shake-up-healthcare.html.

providers make complete electronic health records (EHRs) available to patients.[2] New kinds of health information are being created in the private sector as companies develop different forms of personal health record (PHR) management platforms, including smartphone applications and wearable devices that patients are using to track food consumption, exercise, blood pressure, and a variety of other health metrics.[3]

The government's goal is to "empower individuals and families to invest in and manage their health" by giving them access "to the applications and services that can safely and accurately analyze" their health information.[4] To that end, the U.S. Department of Health and Human Services (HHS) has released rules that authorize providers and patients to designate trusted intermediaries who can access EHRs through open application program interfaces (APIs).[5] This is happening at the same time the entire healthcare system is driving towards value-based care models.[6] Under a value-based system, providers and doctors increase their engagement with patients, reminding them when to take medication or schedule appointments, and predicting when a patient may need medical treatment or intervention in advance.[7]

Trusted intermediaries may facilitate value-based care with user-friendly applications that allow providers and doctors to better engage with patients. Applications may also be the key to a patient-centered model because they can enable patients—and their families and caregivers—to take charge of their own care. In principle, patients could designate trusted intermediaries as digital health advisors.

---

[2] In 2010, under the Health Information Technology for Economic and Clinical Health (HITECH) Act, HHS began incentivizing healthcare providers to transition paper health records to EHRs. *Electronic Health Records (EHR) Incentive Programs*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms (last modified Oct. 6, 2015). The HITECH Act strengthened the HIPAA Privacy Rule by requiring providers to give patient's access to their EHRs. Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5631 (Jan. 25, 2013), (codified at 45 C.F.R. pts. 160, 164).

[3] *See Maintain Your Medical Record*, HEALTHIT.GOV, http://www.healthit.gov/patients-families/maintain-your-medical-record (last updated Mar. 25, 2015). *See also Patient-Generated Health Data*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/patient-generated-health-data (last updated Sept. 30, 2015).

[4] Press Release, White House, Office of the Press Sec'y, Fact Sheet: President Obama's Precision Medicine Initiative (Jan. 30, 2015), https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative.

[5] *See* Meaningful Use Stage 3, 80 Fed. Reg. 62,762, 62,844 (Oct. 16, 2015), (to be codified at 42 C.F.R. pts. 412, 495) and 2015 Edition Health IT Certification Criteria, 80 Fed. Reg. 62,602, 62,603 (Oct. 16, 2015), (to be codified at 42 C.F.R. pt. 170).

[6] Michael E. Porter & Thomas H. Lee, *The Strategy That Will Fix Health Care*, HARV. BUS. REV. (Oct. 2013), https://hbr.org/2013/10/the-strategy-that-will-fix-health-care.

[7] *See* David Blumenthal, *What Health Care Will Look Like in 2030. Maybe.*, WALL ST. J. (Apr. 28, 2015, 7:15 AM), http://blogs.wsj.com/experts/2015/04/28/what-health-care-will-look-like-in-2030-maybe/.

In this role, intermediaries could aggregate and analyze an individual's health information from multiple sources (e.g., various providers and patient-generated health information from PHR platforms) and then engage with patients through their applications to assist in monitoring their health, suggesting potential care plans, or providing other guidance for the patients to discuss with their doctors and providers.

Empowering patients to meaningfully use their health information is a promising development. At the same time, it raises a series of policy challenges. To discuss the changing healthcare information landscape and appropriate policy responses to these opportunities and challenges, the Silicon Flatirons Center convened a group of experts from government, academia, and the private sector on June 17, 2015 for a roundtable discussion under the "Chatham House Rule."[8]

This report, which captures, is informed by, and follows the roundtable discussion, proceeds in three parts. Part I of this report captures the challenges to the healthcare transformation identified by the roundtable participants. In so doing, it highlights how patient and provider culture and behavior creates barriers to information access and describes the privacy and security concerns associated with allowing intermediaries to access patient information. Part II offers policy solutions raised by the roundtable that HHS should consider to address the challenges identified. These solutions include ensuring patient-designated intermediaries are not unreasonably blocked from accessing EHRs, incentivized creation and adoption of a Code of Conduct and Model Privacy Notice, and a fiduciary obligation for digital health advisors. Part III describes the benefits of the proposed policy solutions and how they will facilitate the emerging healthcare transformation.

I. Identifying the Challenges to the Healthcare Transformation

The roundtable participants identified two overarching challenges to the emerging healthcare transformation. First, the participants determined that the culture and behavior of patients[9] and providers[10] creates barriers to information

[8] "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." Chatham House Rule, Chatham House, the Royal Institute of International Affairs, https://www.chathamhouse.org/about/chatham-house-rule#sthash.cZNUwgwH.dpuf (last visited Nov. 14, 2015). Participants were invited to speak as individuals and to express views that may not be those of their organizations. All attributions were included with permission. If not cited, facts or opinions that are reported are those of individual participants and unless otherwise noted, they are not consensus positions. A list of attendees is provided in Appendix A.

[9] This is a general term used to capture individuals as both patients and consumers.

[10] This term is also meant to capture the accountable care organizations (ACOs) with which some providers are affiliated.

access that are stifling the ability of intermediaries[11] to create innovative applications. Second, the participants concluded that we must address privacy and security concerns associated with allowing intermediaries to access health information if we are to benefit from innovation in Health IT.

A. Culture and behavior creates barriers to health information access.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule recognizes patients' control over their health information, including the right to access their complete EHR.[12] But "there is a long distance between policy and reality," as Aneesh Chopra, Co-founder and Executive Vice President of Hunch Analytics put it, noting a range of existing cultural and behavioral barriers to robust health data access.

1. Patients

Patient access to their health information is valuable because today they are in the best position to facilitate the seamless exchange of information between providers and intermediaries, and to make choices about when and with whom data is shared.[13] This promotes adoption of the patient-centered system because intermediaries can develop applications that allow patients to meaningfully use their information. There was a general consensus among the participants that most patients generally want the benefits that flow from increased exchange of their health information. However, there was disagreement about how much patients actually want to access their information and the extent to which they should be forced to engage in a patient-centered system, if they do not do so voluntarily, in order to alter the dynamics within the healthcare system.

Many participants argued that patients desperately want to access their information and use that information to manage their healthcare. According to Mahesh Krishnan, International Chief Medical Officer and Group Vice President of Research and Development at DaVita Healthcare Partners, "patients are getting upset with the quality of their diagnoses." They are asking for their raw health data

[11] Intermediaries include both data intermediaries (third-parties that collect and convey health information to patients) and information intermediaries (third-parties that interpret patient information and serve as digital health advisors to patients). When discussed in connection with EHRs, intermediaries are generally considered applications which patients use to access and aggregate their health information.

[12] Modifications to the HIPAA Rules, 78 Fed. Reg. at 5631.

[13] According to one participant, there are fewer federal and state regulatory hurdles when patients authorize intermediaries to access their information. *See* Karen B. DeSalvo & Lucia Savage, *When and Where You Need It Most: Your Rights to Access and Transmit Your Health Information*, HEALTHIT BUZZ (January 11, 2016, 11:08 am), http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/your-rights-to-access-and-transmit-your-health-information/. *See also Id.* at 5634-35.

so that they can analyze their health history, conduct their own research, seek second opinions, question a doctor's diagnosis, and correct inaccuracies. Another participant suggested that 86% of people who know they can use a health care portal use it.[14] The problem is, most patients simply do not know that they have a right to access their health information.[15] Jamie Grant, Director of National Markets at CareSync, noted that sometimes the "pervasive belief is that the record is exclusively owned by the provider and health system, not owned in conjunction with the patient." Another set of patients do know they have a right to access their information, but do not ask for it. In some cases, this may be because they still believe that obtaining the data is cost-prohibitive.[16] Of the patients that do ask for their health records, some are inaccurately told by providers that the provider is not authorized to share the information with the patient.

Conversely, other participants argued that some patients may not want to access their information or engage in the system. The fact that patients are not asking providers for their EHRs, a few roundtable participants suggested, is indicative not that they are unaware of their rights, but rather that they simply do not wish to exercise them. They questioned whether the emerging transformation is a case of "the tail wagging the dog"—either providers driving for complete patient records or intermediaries motivated to obtain access to patients' information to develop their own business models. These patients are reluctant to adopt a new system where they must allow intermediaries to access their health information for a few key reasons. Some of these patients simply succumb to inertia—they are not concerned with their health until they become sick. Another group of patients in this category simply have a learned behavior to trust the physicians implicitly and do not want to disturb the existing process. Finally, the participants highlighted that some patients are simply averse to adapting to a new patient-centered healthcare system due to a lack of trust in an unknown system and fear that there are inadequate privacy protections. "In

---

[14] However, another study found that 64% of patients do not use portals and of those, only 35% did not know that a portal was available. The remainder knew it was available and chose not to use it. Fred Pennic, *64% of Americans Do Not Use Online Patient Portals*, HIT CONSULTANT (Dec. 16, 2014), http://hitconsultant.net/2014/12/16/64-of-americans-do-not-use-online-patient-portals/.

[15] *See* Alison Diana, *Who Owns EHR Data?*, INFO. WEEK (Sept. 9, 2014, 9:16 AM), http://www.informationweek.com/healthcare/electronic-health-records/who-owns-ehr-data/d/d-id/1307043. *See also* Farzad Mostashari, *Happy Data Independence Day!*, GETMYHEALTHDATA (July 4, 2015), https://getmyhealthdata.org/2015/07/04/happy-data-independence-day/.

[16] With paper health records, costs could be high, but it should be cheaper for providers to duplicate EHRs for patients. A source of confusion may be the differing state laws that regulate how much providers can charge to prepare a patient's health records. *See* Stan Crosley, *HIPAA Privacy Rule Access Right: Assessing Fees When an Individual Requests Electronic Access to PHI*, PRIVACY AND SECURITY WORKGROUP (Sept. 21, 2015), https://www.healthit.gov/facas/calendar/2015/09/21/policy-privacy-security-workgroup. In September, the ONC's Privacy and Security Working Group held two days of hearings discussing the fees charged for patients to access their electronic records. *See* Privacy & Security Workgroup (Sept. 21, 2015), https://www.healthit.gov/facas/calendar/2015/09/21/policy-privacy-security-workgroup; Privacy & Security Workgroup (Sept. 28, 2015), https://www.healthit.gov/facas/calendar/2015/09/28/policy-privacy-security-workgroup. *See also* Diana, *supra* note 15.

America, we regard our health information with a sort of visceral sense of privacy," FTC Commissioner Terrell McSweeny explained. Consequently, people are slow to adopt some technologies until they are convinced that adequate privacy protections are in place—a high bar.

Whether patients engage in a patient-centered health system may simply depend on whether they can access applications that make their information useful. Even though American patients are concerned about privacy, they may find that having the information easily accessible to them, their family members, or their doctors may be the difference between life and death. Shane Green, Co-Founder and CEO of Personal, Inc., suggested that it is even more basic than that. He highlighted a scenario common in the current system—the frustrating task of completing new forms with the same basic personal information for each provider. It turns out that patients are motivated to adopt a patient-centered system when they see that applications can be used to effectively share information and obviate frustrating tasks like this. They quickly value the benefit over their privacy and security concerns, many of which were beyond their comprehension in the first place.[17] In other words, it is not so much the tail wagging the dog as a case of people not knowing what they want until it is made available to them.[18] The challenge that may remain is getting applications to patients who would benefit from them most or when they are most likely to adopt them (i.e. right when they are about to fill out another form).

Grant said that to engage patients, we simply must recognize that they are the only constant in the system and that the fastest path to interoperability is for data to travel with the patient. They will engage if they have understandable and meaningful health data. A major part of that is simply having ownership to all of their personal health information in one useful format and the ability to share the information at their discretion with all stakeholders across the continuum of care. However, many participants expressed concern about the burden this might place on the average patient.[19] Between EHRs and patient-generated health information, complete patient

---

[17] Green said that some patients ask what kind of encryption is in place, but may not even know what kind of encryption is out there. Typically those handling the information are incented to have stronger security controls in place than the average consumer might imagine or recognize.

[18] This comment was in reference to the famous quote by former Apple CEO Steve Jobs that "people don't know what they want until you show it to them." Owen Linzmayer, *Steve Jobs' Best Quotes Ever*, WIRED (Mar. 29, 2006), http://archive.wired.com/gadgets/mac/commentary/cultofmac/2006/03/70512?currentPage=all. A related reference was made to the recently introduced Disney MagicBand. Cliff Kuang, *Disney's $1 Billion Bet on a Magical Wristband*, WIRED (Mar. 10, 2015, 7:00 AM), http://www.wired.com/2015/03/disney-magicband/ ("we tend to acclimate [to new technology] quickly if it delivers what we want before we want it").

[19] According to Carol Diamond, Senior Advisor at Markle, "we've conflated the providers need to share information with the provider sharing information with the patient for the patient's use." She provided an anecdote of a father of a severely ill girl who attended a Markle conference on information sharing in health care. He talked about the two six-inch binders of his daughter's

records are extensive and difficult to meaningfully use.[20] Patients may not be able to comprehend the sheer complexity of the information, let alone aggregate it and analyze it to develop a comprehensive health plan. Even if patients can rely on providers or intermediaries to aggregate, analyze, and create a care plan using their information, they may not know which information is appropriate to share with each party.

Whatever patient engagement can be achieved through increased awareness of their right to their health information and access to applications that allow that information to be meaningfully used, Lucia Savage, Chief Privacy Officer at the Office of National Coordinator for Health Information Technology, concluded that the policies we create must "empower those that want to be empowered without imposing on people who don't want to be imposed on." For patients, the question then remains, what is the right balance between privacy and security versus the ability to have greater control of health outcomes?

2. Providers

Several roundtable participants said that providers are anxious to access patient health information held by patients or other physicians. Providers that can assemble a complete patient health record are in the best position to provide value-based healthcare.[21] Consequently, many providers are frustrated by the barriers to data access. By Chopra's calculation, providers desire information access more than patients, particularly when participating in value-based payment models that reward greater coordination and collaboration. However, because some providers are unwilling to share the information they possess, they are partly to blame for the barriers that are making information access difficult. According to the roundtable, providers may be unwilling to share this information due to liability concerns with sharing HIPAA-protected information (or a lack of understanding of the law).[22] Many

---

medical records he would carry from doctor-to-doctor worried that some part of her complex medical history would be missed in deciding her treatment. He told the audience that he brought the binders with him to every appointment for his daughter, and one doctor said "I wish every patient did this." His response was, "Why is this my job? You can't do this fast enough."

[20] *See* Steve Lohr, *The Healing Power of Your Own Medical Records*, N.Y. TIMES (Mar. 31, 2015), http://www.nytimes.com/2015/04/01/technology/the-healing-power-of-your-own-medical-data.html?_r=2.

[21] In the anecdote highlighted in footnote 19, *supra*, the father was bringing his daughter's medical records to doctor's appointments because he was concerned that different doctors were ordering duplicative services or conflicting drugs that might be dangerous to her. Diamond noted the importance of information sharing so that providers have access to medical history before they order tests, knowing the results from the last physician the patient saw, or knowing what medication the patient is on before prescribing. "Allowing patients to bring information is fine, but it's a poor backstop for the doctor having the information in the first place," she said. *See also* Porter & Lee, *supra* note 6.

[22] Lohr, *supra* note 20.

providers have also adopted a passive system that relies on patients to ask for their information.[23] The business models of other providers may incentivize them to engage in information blocking in an attempt to retain patients or in order to monetize the information they have.[24] Providers may also be unwilling to accept data inputs from patients to correct inaccuracies or in the form of patient-generated data from PHR platforms, if they cannot account for the provenance of the source data.

Chopra shared an anecdote that exemplified the current limitations of data exchange. As an experiment, he and a provider at a health system that held his records from a previous visit attempted to communicate using the DIRECT certified email vendor of Aneesh's choice rather than the one setup by the health system. His email bounced back as an unrecognized address because the Health Information Services Provider (HISP) his email vendor chose did not interconnect with the health system's HISP. The experience reflected what would happen if email from his Gmail account could not reach someone with a Yahoo address. Lisa Hone, Associate Bureau Chief in the Wireline Competition Bureau at the Federal Communications Commission, noted that on top of that, doctors are uncomfortable having that kind of back and forth communication with patients, either due to liability risks or resource concerns. Thus, use of such one-way communications may be intentional even though it may limit the ability of patients to exercise their rights. Given providers' liability concerns about sharing information with patients, it is no wonder they are even more reluctant to share data with intermediaries. In that scenario, providers are not sure if they will be held liable if there is a privacy or security breach with the intermediary.[25] Providers may desire a "seal of approval" or other certification before sharing information with a particular intermediary.

Related to providers' unwillingness to share information, many have adopted a passive system relying on patients to request the information.[26] Even when patients do ask for their records, providers may still make accessing it cost-prohibitive, even though existing laws require the costs be reasonably related to the cost of producing the record, which should be minimal for EHRs.[27]

---

[23] *Id.*

[24] *Id.*

[25] *See Id. See also* PRICEWATERHOUSECOOPERS, HEALTHCARE DELIVERY OF THE FUTURE 6 (2014), http://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/pwc-healthcare-delivery-of-the-future.pdf.

[26] There is no requirement that providers inform patients about their right to access their information, but the participants were highlighting that due to information asymmetry about that right, providers may be in a better position to inform patients that they can request the information.

[27] 45 C.F.R. § 164.524(c)(4) (2014). Grant described a situation where a pediatric patient with a rare disease was told he could have his paper health record for $2,000 and the same information on a CD for $1,000. As further evidence, in October 2015, a class action lawsuit was filed against two Washington, DC-area hospitals alleging excessive fees for electronic records. Mary Butler, *Class Action Lawsuit Alleges Excessive Fees for Copies of Patient Medical Records*. Journal of AHIMA

The participants' concerns about information blocking were highlighted in an ONC report.[28] "Information blocking occurs when persons or entities knowingly and unreasonably interfere with the exchange or use of electronic health information."[29] Providers that engage in information blocking may be trying to monetize the value of the information.[30] Providers can monetize the information by charging fees to access it or by holding onto the information to keep patients from switching to another provider.[31] Providers, or their technology vendors, may also hold this information hostage by restricting access in contract terms, implementing non-standardized APIs that make exchange difficult, or by blocking other parties from accessing their API under the guise of privacy and security concerns.[32] Companies also might engage in this activity if they have sunk costs into creating their own portals or APIs that they are attempting to recover.[33]

Finally, McSweeny put forth a shared sentiment that there is a "gap of people not being able to put their information back into the system in a meaningful way." Patient-generated information and the correction of inaccuracies in a patient's record have the potential to increase the quality of care.[34] Some doctors are unwilling to accept information inputs from patients because it challenges their "doctor knows best" mentality.[35] They are accustomed to relying only on their knowledge, experience, and judgment when assessing a patient. Additionally, because they cannot verify the validity of external data, they may absorb it differently than what the patient tells them in the exam room. One participant questioned this concern of physicians, noting that it is inconsistent for doctors to accept as truth whatever patients write on an intake clipboard, but not accept other patient-provided information. However, Krishnan noted that some doctors embrace incorporating

---

(Oct. 28, 2015), http://journal.ahima.org/2015/10/28/class-action-lawsuit-alleges-excessive-fees-for-copies-of-patient-medical-records/. *See also* Mostashari, *supra* note 15.

[28] OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., REPORT TO CONGRESS, REPORT ON HEALTH INFORMATION BLOCKING (2015), https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf [hereinafter REPORT ON INFORMATION BLOCKING].

[29] *Id.* at 8.

[30] David Brailer, *They're Your Vital Signs, Not Your Medical Records*, WALL ST. J. (Apr. 30, 2015 7:36 PM), http://www.wsj.com/articles/theyre-your-vital-signs-not-your-medical-records-1430436971.

[31] REPORT ON INFORMATION BLOCKING, *supra* note 28, at 13.

[32] *Id.* A more recent report by the Health IT Policy Committee under the ONC emphasized other challenges to the exchange of health information, but still suggested that information blocking was a cause. HEALTH INFORMATION TECHNOLOGY POLICY COMMITTEE, *Report to Congress, Challenges and Barriers to Interoperability* 12, 13-14 (Dec. 2015), https://www.healthit.gov/facas/sites/faca/files/HITPC_Final_ITF_Report_2015-12-16%20v3.pdf.

[33] REPORT ON INFORMATION BLOCKING, *supra* note 28, at 14.

[34] Mary Jo Deering, *Issue Brief: Patient-Generated Health Data and Health IT*, OFF. NAT'L COORDINATOR 8 (Dec. 20, 2013), http://www.healthit.gov/sites/default/files/pghd_brief_final122013.pdf.

[35] *See* Mostashari, *supra* note 15.

patient-generated information because it increases the accuracy of their diagnoses and reduces liability. They are often just overwhelmed by the sheer volume of information, he said.[36] Since they cannot process it on their own, they may welcome intermediaries into the system to help do that. When it comes to inaccuracies in a record, part of the challenge is that it is sometimes just a disagreement between the doctor and patient.[37]

B. Access and use of patient health information by intermediaries creates privacy and security concerns.

Aside from the barriers to information access created by patients and providers, intermediaries are suffering from a lack of trust that they have adequate privacy and security controls when accessing and using the information. The participants identified four specific challenges. The first is defining exactly what constitutes health data today. The participants also discussed privacy and security risks associated with the collection and use of health information by intermediaries. Third, the roundtable discussed how there is no universal code of conduct to mitigate privacy and security risks. Finally, even if there was a code of conduct, the participants were not sure which agency or what mechanism to use for enforcement.

1. Defining Health Information

"We have exhausted the moment where we can talk about health data as health data." That comment by Diamond seemed to be the consensus among the participants. Traditional health data—that which falls under a designated covered entity, such as a health plan or healthcare provider—is addressed by the privacy and security protections of HIPAA.[38] However, HIPAA does not extend to intermediaries unless they are designated business associates of providers (and only then to the information sent by the provider, not all the intermediary's activities).[39] Regardless, most participants agreed that the scope of health information today is beyond the traditional and actually includes any patient-generated data.[40] It was suggested that we can look at a patient's Google searches, Amazon purchases, and the articles they have read, and know exactly what their health concerns are, though not necessarily

---

[36] "Experts estimate that in five years we will generate 50 times more health information than today." Brailer, *supra* note 30.
[37] *See* Diana, *supra* note 15.
[38] CONSUMER REPORTS, BETTER HEALTH CARE: YOUR MEDICAL DATA 14 (2015), http://consumerhealthchoices.org/wp-content/uploads/2015/05/HealthDataGuide-June2015.pdf.
[39] *Id.*
[40] These comments are echoed and documented in a report on Health Big Data that was prepared under a charge from ONC's Health IT Policy Committee. *See* HITPC PRIVACY AND SECURITY WORKGROUP, HEALTH BIG DATA RECOMMENDATIONS (2015), https://www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf.

that the online activity applies to the patient or a family member. Some intermediaries are beginning to use this type of information in preventative care.[41]

2. Privacy and Security Risks With How Intermediaries Collect and Use Information

Despite the benefits, some participants expressed concerns about how intermediaries collect and use patient health and non-health information. Jeff Blattner, President of Legal Policy Solutions, expressed that "when we get to a world where I have my medical history on my flash drive and there's perfect privacy, that still doesn't speak to who can ask for it and what they can do with it once I've voluntarily given it to them." He went on to suggest that if the asking party has market power, the patient may have no realistic alternative but to agree. The concerns about collection and use of data manifested in three ways. First, participants were worried that patients will not know which intermediaries are qualified to aggregate a patient's information and provide beneficial health care guidance, while using reasonable data protection measures. Patients may not have the wherewithal to determine which intermediaries are legitimate and can therefore be trusted.

Second, some expressed concern that inadequate consumer protections mean that intermediaries can use or sell information to the disadvantage of patients. Melissa Goldstein, Associate Professor in the Department of Health Policy and Management at George Washington University, envisioned scenarios where a mortgage lender denies a loan because it had access to the patient's prescription and knew the patient was diabetic; knew that the patient was in marriage counseling and was concerned about long-term income flow; or knew the patient bought a pregnancy test and diapers, assumed the patient was pregnant and was concerned about the patient's expenses. There was also concern about intermediaries asking patients to waive most of their privacy rights through clickwrap agreements that patients rarely read.[42] "If somebody has a privacy policy that they say and then lie about it, the FTC is going to be all over that . . . but if that privacy policy says we're going to take all your data and we're going to sell it to anybody we feel like, we don't have the rules that deal with that," said Kirk Nahra, Partner at Wiley Rein.

---

[41] Kirk Nahra, Partner at Wiley Rein, stated that "one of the ways that some of the health insurers are trying to [predict things like emergency room visits] is by using things like your income level, and number of cars you have, and whether you're married, which is data that no one would ever think of as healthcare data." *See, e.g.,* Natasha Singer, *When a Health Plan Knows How You Shop*, N.Y. TIMES (June 28, 2014), http://www.nytimes.com/2014/06/29/technology/when-a-health-plan-knows-how-you-shop.html?_r=1.

[42] For example, CVS required customers to waive some HIPAA rights if they wanted to participate in a rewards program. Patrick Ouellette, *CVS rewards program requires customers to waive HIPAA rights*, HEALTHIT SECURITY (Aug. 19, 2013), http://healthitsecurity.com/news/cvs-rewards-program-requires-customers-to-waive-hipaa-rights.

Third, the participants were concerned that once an intermediary has access to the patient's information, it may engage in information blocking in an attempt to monetize the information, like some providers or EHR technology vendors.[43] With a growing number of intermediaries, a large amount of health information could be held hostage in many small silos. This outcome would not only hurt patients, but also the budding information intermediary market.

3. No Universal Code of Conduct to Address Privacy and Security Risks

The participants reached consensus that there is no common code of conduct to govern how intermediaries collect and use patient information in order to mitigate privacy and security risks. Nahra said that "for the first time, the gap in HIPAA really matters . . . and we haven't come up with a good set of rules." Because of the limited definition of health data, many agreed that folding in modern data sources under the existing HIPAA framework was impractical. HIPAA was enacted when the healthcare industry was static and covered entities clearly dealt with health information.[44] Creating a new set of HIPAA-like regulations specifically for these new data sources was also not favored because it may not allow the type of information exchange that will support better health outcomes and patient engagement.

The evolving healthcare industry requires a new set of rules. One suggestion was to identify the norms in the current marketplace, validate those norms, and then identify and fill any gaps. That is potentially a suggestion that intermediaries would support. From their perspective, they are self-regulated entities because their entire business model is built on maintaining the privacy of patient information. However, others believe intermediaries are motivated more by how they can use the information than by protecting patient privacy. Regardless, regulations might actually legitimize the privacy and security controls on intermediary applications helping them overcome patient skepticism. Some participants suggested that intermediaries implement the Fair Information Practice Principles (FIPPs).[45] The FIPPs framework would ensure that all information collected and used by

---

[43] The ONC report noted that "most complaints of information blocking are directed at health IT developers . . . that [] charge fees that make it cost-prohibitive for most customers to send, receive, or export electronic health information." REPORT ON INFORMATION BLOCKING, *supra* note 28, at 15.

[44] *Moving Toward a New Health Care Privacy Paradigm*, Wiley Rein LLP (Nov. 2014), http://www.wileyrein.com/newsroom-newsletters-item-5151.html.

[45] *Privacy and Security Tiger Team Annual Executive Summary*, U.S. DEP'T OF HEALTH & HUMAN SERVS. 2, https://www.healthit.gov/sites/default/files/tigerteamannual_hit_executive_summary.pdf (last visited Oct. 23, 2015). In fact, the ONC has already created a FIPPs-based framework for exchanging health information. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., NATIONWIDE PRIVACY AND SECURITY FRAMEWORK FOR ELECTRONIC EXCHANGE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (2008), https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

intermediaries is done so in a way that protects the privacy of the patient.[46] Another suggestion was for intermediaries to adopt a voluntary code of conduct. In addition to the development of rules and responsibilities governing the use of patient information by intermediaries, the ONC Model Privacy Notice was suggested as a way to provide transparency as to the privacy and security practices that intermediaries have actually adopted.

4. Uncertain Enforcement Mechanism

Even with an adequate code of conduct in place, the participants expressed uncertainty about how it would be enforced. FIPPs does not specify how its standards should be enforced when, such as this case, intermediaries do not comply with them. Many supported ensuring a robust and transparent code of conduct is in place and then relying on the FTC to enforce whatever privacy protections are established. However, there was some concern that patients may not know what to look for in order to take advantage of the FTC's enforcement capabilities.

II. Policy Solutions to Address the Identified Challenges

Government initiatives have created the drive and foundation for a patient-centered model of care, but policymakers should consider additional solutions to address the challenges and further facilitate the healthcare transformation. The roundtable discussion and participant suggestions led to three policy solutions that address the challenges and adjust the incentive structure to facilitate the transformation. First, policymakers should ensure that there are adequate processes in place to prevent providers from circumventing rules that allow patient-designated intermediaries to access a patient's EHR. Second, policymakers should incentivize the creation and adoption by intermediaries of a Code of Conduct and adoption of the Model Privacy Notice. Third, policymakers should create controls to ensure that digital health advisors have a fiduciary obligation to patients.

A. Ensure adequate processes are in place to review allegations of providers blocking access to EHRs by designated intermediaries.

The 2015 Edition Health IT Certification rule[47] (Certification rule) and Meaningful Use Stage 3 rule[48] (MU3 rule), both released in October 2015, go a long way towards addressing many of the challenges identified by the roundtable participants with regard to access to EHRs. The certification standards set out in the

[46] *Fair Information Practice Principles, Introduction*, IT LAW WIKI, http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles (last visited Oct. 23, 2015).
[47] 2015 Edition Health IT Certification Criteria, 80 Fed. Reg.
[48] Meaningful Use Stage 3, 80 Fed. Reg.

Certification rule apply to both provider APIs and third party APIs.[49] The rule requires a demonstration that all APIs, respond to specified data requests before they can be certified—in short, the APIs must be open.[50] The MU3 rule allows providers to designate at least one intermediary that can access a patient's EHR.[51] It also supports "a patient's right to have his or her protected health information sent directly to a third party designated by the patient consistent with the provision of access requirements" of the HIPAA Privacy Rule.[52] The rule further specifies that designated third parties can access a patient's EHR so long as it meets the technical and security specifications of the provider's API.[53] Providers are expected to provide detailed instructions on how to access and leverage the API.[54]

The only shortcomings of the rules may be if providers fail to provide detailed information, block designated third-party APIs under the guise of a technical or security concern, or otherwise use strategies to slow the access to the information. Under these circumstances, the patient may, in practice, have no choice but to rely on a provider-designated intermediary that has an incentive to cater more to the provider's interests than the patient's. Policymakers should ensure there are adequate processes in place to receive complaints from patients and certified third parties alleging such practices by providers and timely review those practices.

B. Incentivize the creation and adoption by intermediaries of a Code of Conduct and use of the Model Privacy Notice.

Policymakers should incentivize intermediaries to create and adopt a Code of Conduct, as well as incentivize intermediaries to use ONC's Model Privacy Notice (MPN). In this context, a code would outline the rules and responsibilities of intermediaries handling patient information while a notice would serve as a transparent explanation of the rules and responsibilities that each intermediary has adopted. If used together by intermediaries, they would provide enforceable standards, effectively making the code binding. There is currently not a binding and enforceable code for health information intermediaries—they have not taken it upon themselves to develop and adopt a code. In addition, few intermediaries have made use of the existing MPN to make transparent their existing practices, despite the notice being in the public domain and thus available for intermediaries to adopt,

---

[49] *See* 2015 Edition Health IT Certification Criteria, 80 Fed. Reg. at 62,604 *and* Meaningful Use Stage 3, 80 Fed. Reg. at 62,871.
[50] 2015 Edition Health IT Certification Criteria, 80 Fed. Reg. at 62,603.
[51] Meaningful Use Stage 3, 80 Fed. Reg. at 62,844.
[52] *Id.* at 62,843. HIPAA Privacy Rule provision of access requirements generally require providers to give patients access to their information in the form requested in a timely manner and at a reasonable fee. 45 C.F.R. 164.524(c).
[53] Meaningful Use Stage 3, 80 Fed. Reg. at 62,842.
[54] Meaningful Use Stage 3, 80 Fed. Reg. at 62,842.

adapt, and build on.[55] Policymakers could incentivize intermediaries to take action or risk binding regulations that have the potential to stifle access to information in the search for perfect privacy and security. Use of the MPN could be incentivized in a similar fashion. Policymakers could even consider making adoption of the Code and MPN part of the certification process for intermediaries.

With the incentive in place, a "coalition of the willing" could be formed by industry stakeholders to create a code that safeguards the collection and use of patient information while also facilitating information exchange. The ONC formed a task force to identify the actual privacy and security concerns specific to APIs developed in the health data exchange.[56] When complete, intermediaries could use the findings of the task force to design a code that addresses the concerns or, again, risk regulation that does so. A successful code developed in the private sector is not unheard of. The Network Advertising Initiative developed a "Self-Regulatory Code of Conduct" to govern data collection and use for digital advertising.[57] In the education space, the "Student Privacy Pledge" has seen widespread adoption,[58] which was accelerated after it was endorsed by President Obama.[59] In this case, the incentive provided by the risk of regulation would serve to promote adoption. Further, a code based off the FIPPs standards could address privacy and security concerns while potentially avoiding shortcomings in the student pledge.[60] For example, the FIPPs use limitation would prevent harmful use of patient information by preventing intermediaries from using or selling information outside of how they previously specified; the data minimization standard would prevent accumulation of unnecessary information; and the security principle would ensure intermediaries are taking necessary steps to protect the information.[61] Since FIPPs were designed to balance privacy interests with market development, this all could be achieved without limiting the benefits of the developing intermediary market.[62]

---

[55] *See, e.g., What To Do With Your Data*, GETMYHEALTHDATA, http://getmyhealthdata.org/home/using-your-data/ (last visited Oct. 23, 2015).
[56] *FACA Workplan*, HEALTH IT POLICY COMMITTEE 4 (Oct. 6, 2015), https://www.healthit.gov/facas/sites/faca/files/Joint_HIT_FACA_work_2015-10-06.pdf.
[57] *About the NAI*, NETWORK ADVERT. INITIATIVE, https://www.networkadvertising.org/about-nai/about-nai (last visited Oct. 23, 2015).
[58] Press Release, Software & Info. Indus. Ass'n, Student Privacy Pledge Crosses Milestone with 100 Signatories (Feb. 4, 2015), http://www.siia.net/Press/Student-Privacy-Pledge-Crosses-Milestone-with-100-Signatories.
[59] Press Release, Student Privacy Pledge, President Obama Endorses Student Privacy Pledge (Oct. 7, 2014), http://studentprivacypledge.org/?page_id=213.
[60] Natasha Singer, *Data Security Gaps in an Industry Student Privacy Pledge*, N.Y. TIMES (Feb. 11, 2015), http://bits.blogs.nytimes.com/2015/02/11/data-security-gaps-in-an-industry-student-privacy-pledge/?_r=0.
[61] *National Strategy For Trusted Identities In Cyberspace, Appendix A – Fair Information Practice Principles (FIPPs)*, NIST, http://www.nist.gov/nstic/NSTIC-FIPPs.pdf (last visited Oct. 23, 2015).
[62] IT LAW WIKI, *supra* note 46.

Furthermore, the ONC should incentivize use of the MPN and consider working with stakeholders to update the MPN. The notice was created by ONC to provide "consumers with information regarding a PHR company's data sharing and data security practices."[63] The "[n]otice is meant to provide information to consumers in a uniform layout they can understand, compare, and use to make an informed decision on which PHR they would like to use."[64] In this context, intermediaries that adopt the Code of Conduct would then make use of the MPN to represent to consumers that they have adopted the Code. It is not clear why the MPN has not been widely adopted; it could be poor engineering, content that is unattractive developers, inertia, or a lack of knowledge by developers that the MPN exists. While the Code of Conduct is being developed, the ONC should seek input from stakeholders on whether the MPN should be updated before its use is incentivized.

Where intermediaries have adopted the Code of Conduct and used the MPN to make that adoption transparent, that would provide grounds for the FTC to enforce the Code on the intermediaries, giving patients confidence that it is not a set of empty promises.[65]

C. Create a fiduciary obligation for digital health advisors.

Policymakers should establish controls to ensure intermediaries serving as digital health advisors have a fiduciary obligation to their patients. In a patient-centered healthcare system, healthcare strategies are increasingly placed in the hands of individual patients. A subset of intermediaries are emerging to serve as digital health advisors for patients.[66] These intermediaries assist patients with interpreting their voluminous health information, identifying risky prescription combinations, selecting doctors, and suggesting comprehensive care plans.[67] Because these intermediaries are playing a more significant role in patient care, an updated model privacy framework may be inadequate to address the risks that flow from this added responsibility. This is particularly the case for certain health advisors that may have conflicts of interest. For example, advisors employed by providers may be compelled to cater more to the provider's interests than the patient's. Fiduciaries

---

[63] HEALTHIT.GOV, *PHR Model Privacy Notice Implementation Guide* 2, https://www.healthit.gov/sites/default/files/phr-model-privacy-notice-implementation-guide-final.pdf (last visited Oct. 23, 2015).
[64] *Id.*
[65] *Enforcing Privacy Promises*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Oct. 23, 2015).
[66] *See, e.g.*, OPTUM, HEALTH CARE ADVISOR (2014), https://www.optum.com/content/dam/optum/resources/whitePapers/heath-care-advisor-WP-0512.PDF.
[67] *Id.* at 9-10.

have a duty to act in the patient's best interest,[68] so a fiduciary obligation would create the necessary safeguards for patients and provide certainty as this submarket develops.

The 401(k) market demonstrates the risks when individuals in advisory positions do not have a fiduciary obligation. When United States companies shifted from pension plans to 401(k)s, retirement investment strategies were put in the hands of individuals.[69] Stock brokers stepped in to advise and assist individuals with this highly complex undertaking.[70] In some situations, a broker has an incentive to advise clients to make investment decisions that benefit the broker's bottom line at the expense of annual returns to their client.[71] The negative consequences of this conflicted advice are magnified when the brokers are assisting individuals with their retirement livelihood. Many consumers are not aware of these potential conflicts, so external standards must be imposed to achieve the necessary protection.[72] In February 2015, the president backed new rules to address this conflict of interest.[73] Under the proposed system, stock brokers would have a fiduciary obligation to their clients; an obligation to make decisions that are in the best interest of the client.[74] Policymakers should preemptively address similar risks in the emerging digital health advisor market.

III. How Adopting the Proposed Policy Solutions Addresses the Identified Challenges to the Healthcare Transformation

The proposed policy solutions ensure patients and ultimately intermediaries can access patient information. Standard intermediaries become trusted intermediaries when they are certified, they adopt the Code of Conduct and make that adoption known by using the Model Privacy Notice, and they comply with fiduciary obligations when serving as digital health advisors. Adoption of the Code helps avoid circumstances where intermediaries ask patients to legally waive all their rights. Use of the notice would give consumers transparency about which intermediaries have adopted the Code and which have not. Overall, the environment created with the policy solutions in place facilitates the development of a robust health application market by these trusted intermediaries. This market will serve to

---

[68] *See generally* Joshua D. Margolis, *Professionalism, Fiduciary Duty, and Health-Related Business Leadership*, 313 J. AM MED ASS'N 1819 (2015), http://jama.jamanetwork.com/article.aspx?articleid=2290657.

[69] EXEC. OFFICE OF THE PRESIDENT, THE EFFECTS OF CONFLICTED INVESTMENT ADVICE ON RETIREMENT SAVINGS 4 (2015), https://www.whitehouse.gov/sites/default/files/docs/cea_coi_report_final.pdf.

[70] *Id.* at 5-6.

[71] *Id.* at 6-7.

[72] *Id.* at 7

[73] Andrew Ackerman & Karen Damato, *Obama Backs New Rules for Brokers on Retirement Accounts*, WALL ST. J. (Feb. 23, 2015, 6:39 PM), http://www.wsj.com/articles/obama-to-back-new-rules-for-brokers-on-retirement-accounts-1424689201.

[74] *Id.*

address the remaining challenges and ultimately facilitate the next stages of the healthcare transformation.

The inability to access patient health information is a substantial barrier to a robust patient-centered health application market. By unlocking health information through open APIs, intermediaries have the tools and incentives to develop applications to serve patients. Current rules allow patients to designate any certified intermediary to access their health information and so long as there are adequate processes in place to review interconnection decisions by providers, information blocking by providers and intermediaries will be reduced, preventing information from reaching a patient-designated endpoint.

The applications market will serve as a natural tool to educate patients and providers about their rights and obligations regarding health information access. It is in the interest of the intermediaries, particularly in a competitive market, to advertise their applications to patients, because they are in the best position to facilitate the intermediary's access to the patient's information. The advertising necessarily informs patients that they have a right to access their information, that they should be able to access the information at a reasonable price, and that they can designate intermediaries to make use of the information. Educated patients and the growing applications market will negate concerns that providers are not taking the opportunity to inform patients of their right to access their information.

Competition in the applications market will drive the development of tools that fully facilitate the meaningful use of health information by patients. Given historical trends in the applications market, it may only be a matter of time before one or two applications become "must-have" applications by patients. The popularity of these applications and the network effects (if used by patients and providers, and connected with other applications) will drive their adoption. This will further help overcome the challenge of engaging patients in the patient-centered healthcare system, especially as patients come to value the benefits over privacy and security concerns.

Patients and providers that remain concerned about privacy and security will find comfort in the Code of Conduct that is adopted, the Model Privacy Notice that would make the Code's adoption known, and fiduciary obligations. Most importantly, intermediaries that adopt the Code will actually protect the privacy and security of patient information, but there are several other benefits. First, these may serve as the "seal of approval" that providers desire to reduce liability concerns about sharing information with intermediaries. Second, the transparency of the Code's adoption provided by use of the MPN will allow patients and providers to identify trusted intermediaries from standard intermediaries. Third, because patients and providers will more likely favor intermediaries that have adopted these controls, they will also effectively limit the number of applications in the market to those that make the effort to comply with them. In turn, patients and providers will be less burdened when

researching applications and innovative applications will be incentivized to enter if there is a greater chance they can distinguish themselves in the market.

For patients that want to access and use their information, the current designation rule with processes to prevent information blocking will make it easier for them to designate the intermediary of their choice. The competitive applications market means that consumers will have more options. These options reduce the conflict of interest associated with provider-designated intermediaries that may have an incentive to cater to the provider's interests over the patients. Patients that do not wish to designate an intermediary would be under no obligation to do so. They can still rely on a provider-designated intermediary (or none at all) and further choose not to access that information or otherwise engage in the patient-centered model. Instead, patients can rely on existing ways that HIPAA supports treatment and movement of data among providers.

A fiduciary obligation for digital health advisors created by policymakers will provide an avenue to prevent patients and providers from being overburdened with trying to meaningfully use the voluminous health information on their own. The advisors will be able to aggregate and analyze information from a variety of sources to identify conflicting prescriptions and help patients and providers coordinate care. This includes information inputs from patients, which lifts barriers created when doctors cannot or do not want to consider patient-provided information. Consequently, patients would have an avenue to correct errors in their records, particularly if intermediaries can crunch the information to determine the likelihood of an inaccuracy. Finally, this increased access and exchange of information will help ensure that providers are fully aware of a patient's complete medical history before providing services, ultimately increasing a patient's quality of care.

Conclusion

The promise of a patient-centered health system is dependent on the ability of intermediaries to access patient information in order to develop applications that allow patients to meaningfully use their information. Government initiatives have been driving this transformation, but if new policies do not address identified challenges, they threaten to stop the transformation in its tracks. Specifically, patient and provider culture and behavior is throwing up barriers to information access by intermediaries. Yet, even if intermediaries had ready access to the information, lingering privacy and security concerns caution against putting the information in their hands. To address these concerns, policies should ensure that providers do not engage in information blocking with patient-designated intermediaries, incentivize the creation and adoption of a Code of Conduct and the Model Privacy Notice, and establish a fiduciary obligation for digital health advisors. Together, these solutions will shift incentives and directly address the concerns identified by the roundtable participants by facilitating the development of a competitive market of trusted

intermediary applications thereby driving adoption of the patient-centered healthcare system.

Appendix A: Participants

Mark Alderman, Chairman, Cozen O'Connor Public Strategies
Jeff Blattner, President, Legal Policy Solutions, PLLC
Doug Brake, Telecommunications Policy Analyst, Information Technology and Innovation Foundation
Jonathan Cedarbaum, Partner, Wilmer Cutler Pickering Hale and Dorr LLP
Aneesh Chopra, Co-founder and Executive Vice President, Hunch Analytics, LLC
Carol Diamond, Senior Advisor, Markle
Jeff Dygert, Executive Director, Public Policy, AT&T
David Edelman, Special Assistant to the President for Economic & Technology Policy, The White House, National Economic Council
Ed Felten, Deputy U.S. Chief Technology Officer, The White House, Office of Science and Technology Policy
Melodi Gates, Senior Legal Editor, Intellectual Property & Technology Service, Thomson Reuters
Ahaviah Glaser, Managing Director, Cozen O'Connor Public Strategies' Health Care Practice
Paul Glist, Partner, Davis Wright Tremaine LLP
Melissa Goldstein, Associate Professor, Department of Health Policy and Management, George Washington University
Jamie Grant, Director of National Markets, CareSync
Shane Green, Co-Founder and CEO, Personal, Inc.
Leslie Harris, Former President, Center for Democracy & Technology (CDT)
John Heitmann, Partner, Kelley Drye & Warren LLP
Lisa Hone, Associate Bureau Chief, Wireline Competition Bureau, Federal Communications Commission (FCC)
Hank Kelly, Partner, Kelley Drye & Warren LLP
Gene Kimmelman, President and CEO, Public Knowledge
Linda Kinney, Senior Advisor for Internet Policy, Office of the Assistant Secretary, National Telecommunications and Information Administration (NTIA)
Mahesh Krishnan, International Chief Medical Officer and Group Vice President of Research and Development, DaVita Healthcare Partners
Chris Laughlin, Student, University of Colorado Law School
Terrell McSweeny, Commissioner, Federal Trade Commission (FTC)
Kirk Nahra, Partner, Wiley Rein LLP
Jon Nuechterlein, General Counsel, Federal Trade Commission (FTC)
Jules Polonetsky, Executive Director, Future of Privacy Forum
David Redl, Chief Counsel, Communications and Technology, House Energy and Commerce Committee
Dana Rosenfeld, Partner, Kelley Drye & Warren LLP
Brad Rostolsky, Partner, Reed Smith
Jocelyn Samuels, Director, Office for Civil Rights, U.S. Department of Health & Human Services (HHS)
Lucia Savage, Chief Privacy Officer, Office of National Coordinator for Health Information Technology, U.S. Department of Health and Human Services
Nick Sinai, Venture Partner, Insight Venture Partners
Phil Weiser, Dean and Silicon Flatirons Executive Director, University of Colorado Law School