U.S. Senate Committee on Health, Education, Labor, and Pensions
Implementing the 21st Century Cures Act: Making Electronic Health Information Available to Patients and Providers
March 26, 2019

Testimony for Lucia C. Savage, JD

Chairman Alexander, Ranking Member Murray and the entire Committee: Thank You for the opportunity to submit these detailed written comments. Part 1 includes the remarks I made as testimony before the Committee. Part 2 adds some important details on how Omada operates as a health care service provider under HIPAA and how ONC's proposal will in many ways help us grow. It also provides some additional detail on the areas where we think ONC could do better.

Part 1:

From October 2014 through January 2017, I served as the Chief Privacy Officer at the Office of the National Coordinator for Health Information Technology. I was the senior privacy advisor for efforts to enable patients to get copies of their health information through apps, and I provided technical assistance as 21st Century Cures was being drafted.

After leaving ONC, I joined Omada Health, a late-stage, privately-held health company focused on chronic disease prevention and management, as well as supporting those dealing with anxiety and depression. We utilize a secure digital communications platform to connect individuals to professional coaches. In the process, our participants share their health information, just as they would with any healthcare provider. We analyze that data in real-time using proprietary data science techniques, and feed actionable insights back to the participant and his or her coach. The result is health care services that adapt in real time to the needs of individual participants, while maintaining the ability to scale quickly and leverage those individual insights at a population health level. One of my duties is to oversee Omada's operations as a healthcare service provider and HIPAA-covered entity, legally just like a doctor's office under federal law. This means that all of the HIPAA Privacy, Security, and Breach Notification rules apply to us.

ONC proposes bold reforms that could significantly impact the way personal health facts are shared and that should foster innovation. Among the most impactful is that information blocking rules apply to health information technology operating in a business-to-business environment. This is a logical, and necessary next step in achieving the vision of an innovative healthcare system where health facts can flow appropriately and securely to benefit patients. Included in my supplemental materials is an article published yesterday in the American Bar Association's Antitrust Law Journal, where Professors Martin Gaynor, Julie Adler-Milstein and I examine the anti-competitive aspects of the B2B health information exchange absent ONC"s rule.

However, there are three issue areas where either ONC could push this vision more aggressively, or where the agency may want to consider unintended consequences from its rulemaking.

First, while the ONC rule strikes a good balance on privacy and security, with appropriate exceptions for privacy promises made to individuals, state or other federal law, securing one's own system, system maintenance, and safety, the rule proposes ongoing deference to organizational policies that might be at odds with democratically-developed privacy laws that support interoperability. I encourage ONC to consider a transition or sunset period, during which institutions have time to adapt to app-enabled authorized sharing of health facts, and to eliminate organizational policies that block the free flow of health information.

Second, the 21st Century Cures Act applies the prohibition against information blocking to developers of "health information technology" as defined in HITECH Section 13101(5). The ONC proposal, however, applies only to a subset of this category, certified electronic health records developers. This limitation leaves out many types of health information technology where individuals' health facts are collected. For example, the proposed rule does not reach to health information technology in the emerging world of connected devices or Software as a Medical Device, and seems to omit any non-certified EHR, such as a lab or pharmacy electronic records system that is not certified.

Third, ONC proposes to allow technology developers to license “interoperability elements.” Licenses must not be so expensive or restrictive as to stifle innovation or create barriers to entry. As ONC finalizes the concept of interoperability elements, it is critical that it clarify that <u>health facts</u> themselves are <u>never</u> to be licensed. Omada made this point in our recent response to the RFI from the Office of Civil Rights; I have also included that comment letter in my supplementary materials.

Finally, I applaud CMS’ efforts to ensure that people have the same app-enabled access to their health facts from plans as from providers. CMS “expects” that “common consumer tools” like laptops, smartphones and apps will be used throughout the healthcare system (84 Fed. Reg. 7628 (March 4, 2019). In the healthcare start up world, we use these “common consumer tools” every day to connect with, and deliver valuable health care services to, individuals. We are excited to have barriers to interoperability fall and we look forward to the time when barriers fall to being paid for efficacious health care services deployed with common consumer tools.

Thank you again for the opportunity to testify. I look forward to answering your questions.

Part 2:

A: Omada Is a Provider and Covered Entity under HIPAA

Despite our digital communications and data science platform, Omada is and operates as a health care service provider under federal law, and thus as a covered entity under HIPAA. Additional detail is set forth below.

HIPAA applies to three types of "providers" (45 CFR 160.103): acute inpatient hospitals, professionals, and "any other entity that supplies health care services and bills electronically for them. The regulation states:

> *Health care provider* means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business [Emphasis added].

Omada falls into that third category, and has operated as a provider and covered entity since its founding in 2011.

As a provider and covered entity, we are legally just like a doctor's office or hospital. This means that when we collect, use, or disclose an individual's health information, we do so under HIPAA's exacting standards. Further, because of how seriously we take our participant's privacy, and as our Terms of Use, Privacy Policy and HIPAA Notice of Privacy Practices make clear, we do not sell data from our participants, even in a de-identified form. So, we are quite distinct from an array of social media and retail apps. The same is not true for an app purchased from an app store that is not offering a reimbursable health care service. In some ways, it is good that as a nation we are having a debate about these ad-tech based apps and privacy at the same time that we are bringing the automation of apps to traditional healthcare. This is because the debate itself raises consumer awareness and that awareness makes sure they are choosing health care modalities that are right for them.

For us, HIPAA's approach to privacy, health fact sharing, and interoperability have enabled us to build a business based on delivering demonstrable health outcomes -- then charging our customers based on those outcomes. Put simply, if we don't deliver improved care, better outcomes, and value to our customers, our business does not work.

For example, for our flagship Diabetes Prevention Program (DPP) healthcare service, the Centers for Disease Control (which oversees recognition standards for DPP) identifies weight loss as the core clinical indicator of success. In our DPP, after paying an initial account set up fee, Omada is paid for its services only if it can prove weight loss. Our outcomes-based model for this program therefore depends on our ability to use the health information we collect from our participants to measure outcomes. It also depends on our ability to share those outcomes, sometimes in an identifiable way, with the organization paying for our health care service, such as a health plan, a clinic, or a self-insured employer. We detailed some examples of our information sharing practices in our response to OCRs recent Request for Information. I have attached that response to this detailed statement.

Given our business model, we already exchange health information regularly where we are legally permitted to do so and it is appropriate, even in a B2B transaction; for example, reporting book-of-business results back to a large health plan via a custom, secure reporting feed or even an API we develop. We believe ONC's push into B2B transactions will facilitate more, and easier, less expensive, secure transactions with a wider variety of business partners, allowing Omada to grow in new ways.

In the past, we declined to be an authorized app within the app store of various certified EHR vendors because we concluded that the price tag was too high and the information terms were too constrained. For example, as a health care provider in our own right, if we acquire a health fact like a blood sugar test result from another provider, we cannot be in a position where we cannot use that fact in our outcomes-based model, or cannot disclose that health fact to other providers or to the individual without paying more fees. We think that ONC's proposal will go a long way towards solving this particular problem, so long as the EHR developer's ability to license "interoperability elements" prohibits attempts to license health facts.

B: Health Facts vs. "Interoperability Elements": As a health care service provider who develops our own software to deliver our services, we handle PHI in ways quite different from traditional healthcare. For example, our intake questionnaire and clinical screener is filled out 100% online, not through a clipboard in a waiting room. This means, however, that from a software engineering and health care services perspective, we have a keen sense of what in our entire database is a meaningful health fact (a person's weight for example) and is not meaningful because it is a piece of metadata (the log file of the scale manufacturer showing it sent the scale weight to us for example). And, we could share just health facts with a person or another business (such as raw data in a spreadsheet sent securely) or we could share those health facts in a more meaningful, structured way.

At Omada, we think ONC means for the "interoperability elements" to be like the meta data or the external structure to the health facts in the examples above. We are all-in on interoperable health facts. And we hope that other health information technology developers of all kinds would be too. But, because ONC's rule imposes few limits on the scope of a license to "interoperability elements," and does not state that health facts are not licensable, we worry that technology developers will license an "interoperability element" only when it is in their self-interest to do so, not for the good of the patient. Worse, a health information technology developer might only license "interoperability elements" in anti-competitive ways. In fact, in writing the accompanying article for the American Bar Association Antitrust Law Journal, my co-authors and I discuss how under Supreme Court precedent, health facts occur in nature and therefore cannot become a single entity's intellectual property.

We also have talked to other health start-ups of various sizes and they share our concern that the proposal to license "interoperability elements" is potentially the exception that undermines the overall goal of interoperability.

C: What Health Information Technology Does ONC's Proposal Cover? In my oral testimony, I described the fact that ONC's proposal does not cover all health information technology. I would like to elaborate.

21st Century Cures amended prior definitions of the Health Information Technology for Clinical Health Act (HITECH) by adding a definition of "interoperability" that applies without exception to all "health information technology," also as defined in HTECH. HITECH section 3000(1) has one definition of "certified electronic health records technology" and a separate and distinct definition of "health information technology" (Id.). "Health Information Technology is

> ''(5) . . . hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information."

Cures applies its definition of "interoperability" and its concomitant prohibition against information blocking to "health information technology", not just to certified EHRs. Cures states:

> ''(10) INTEROPERABILITY .—The term 'interoperability', with respect to health information technology , means such health information technology that—
>
> > ''(A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;
> > ''(B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
> > ''(C) does not constitute information blocking as defined in section 3022(a).''
> > [Emphasis Added. P. Cures section 4003(a)(2)(10), P. Law 114-255 (December 163, 2016) , codified at 42 USC 300jj–52.

Cures then goes on to state that information blocking is prohibited:

> (B)(i) if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; [Id. section (3022(a)(1)(B)(1). [Id. creating section 3022 of the Public Health Service Act. Emphasis added]

Cures then charges ONC with developing rules about what does not constitute information blocking, and that charge is not limited to ONC's traditional regulatory authority over certified EHRs. Rather, that charge states:

> ‘‘(3) RULEMAKING.—The Secretary, through rulemaking, shall identify reasonable and necessary activities that do not constitute information blocking for purposes of paragraph (1).

And it is paragraph (1)(B)(i) that applies the term information blocking to “health information technology.”

Based on the above provisions, Omada believes that Congress in Cures authorized rules against information blocking that reach beyond certified EHR developers. In contrast, ONC”s rule, as proposed, applies only to certified EHR developers, on whom is imposed the certification obligation of developing the open-specification read-only APIs, using the Fast Health Interoperability Resource (FHIR) standard (see generally 84 Fed. Reg. 7465-7508. March 4, 2019). As a result of comparing Cures to ONC’s rule, we concluded that many collectors and custodians of digital health facts are not prohibited from information blocking. Two potential examples follow:

Example 1: A pathologist uses a proprietary health information technology system developed for her by a third party to store lab data. That health information technology system is not certified. The developer is not required to make a standards-based API available for the pathologist’s information sharing needs.

Example 2: A manufacturer sells a leg brace that contains a radio frequency chip and a gyroscope, to measure mobility and gait after a joint replacement. That manufacturer’s proprietary health information technology system that is not certified. Even if the manufacturer bills Medicare for monitoring services and therefore is a HIPAA covered entity, that proprietary health information technology system is not required to make the health facts it contains available to individuals, their physicians or their other providers in a standards-based, interoperable manner.

We recognize that ONC or the Office of Inspector General might not have the robust authorities over health information technology developers that already exist over certified EHR developers. But we see this as an enforcement authority problem to be solved next, not as a reason NOT to extend the prohibition against information blocking to all developers of health information technology. If we truly want interoperable health facts to flow where the individual needs them to manage their care using common consumer technologies (84 Fed. Reg. 7628, March 4, 2019), then information blocking of health facts must be prohibited everywhere.

D: Privacy Policies vs. Privacy Laws: In my testimony, I expressed concern with ONC's proposal to allow organizational policies enacted transparently before ONC"s rule took effect, to continue to be enforced without constituting information blocking. See proposed 45 CFR 170.202(b). There are many organizational policies which are necessary for appropriate privacy practices, and in fact HIPAA requires that covered entities have written policies. We have many at Omada. But all organizational policies are not created equal, and ONC"s rule should not give deference to policies that unnecessarily thwart interoperability. Here are two examples of such policies that should not be allowed to persist.

Example 1: Although the physician's office offers its patients secure identity credentials to message their doctors through their certified EHR, their organizational policy prohibits individuals from asking for a copy of their own health records using the portal. Rather, if an individual does this, office staff requires that the individual contact by fax or mail a remote health information management office. *Bitter [Release of Information] Irony*, Journal of AHIMA November/December 2017, page 32: http://www.ahimajournal-digital.com/ahimajournal/november_december_2017?pg=33#pg33.

Example 2: A hospital system has a written policy that it will not allow individuals to transmit (or download a copy of) their health facts to any technology service that is not approved by the system's information security office, even though there is no evidence that this type of download threatens the security of the hospitals' systems.

ONC's proposal does require that historic policies meet a facts-and-circumstances test for reasonableness, being carefully tailored, etc. But this refinement fails to account for the world we have now, where the full efforts of Congress and the Executive Branch are working to ensure consumers can use everyday technology to manage their health, yet faxes remain ubiquitous. In this situation, it would be far better for patients and their everyday technologies if ONC and HHS required providers to sunset old policies by the effective date of the rule, and to replace them with policies that actually meet the prohibition against information blocking, instead of investigating policy by policy the facts and circumstances of each situation, while patients and their caregivers are waiting for their health facts.

D: Which Providers Does ONCs Proposal Cover? Before concluding I want to be clear that, as proposed, ONC's rule would not apply to Omada Health, because ONC proposes that the only providers within the rule's scope are those identified in the Social Security Act, not entities who, like Omada, fall into that third category of "any other" health care service provider. ONC has requested input on this point, and Omada expects to comment that ONC should use the HIPAA definition of health care provider so that providers of healthcare services of all types cannot block the appropriate interoperable flow of health facts to other providers. We recognize this change will sweep Omada and many others into the ambit of the ONC rule, and we are okay with that. As a health care service provider who uses digital health information to provide personalized services to individuals and to prove our value proposition to payers paying for those services, and with a company value of #ParticipantsFirst, we want to make it easy for our participants to get the healthcare that is right for them, even if it means taking health facts we collected and sharing those facts with another provider.

Respectfully submitted,

Lucia C Savage

Lucia C. Savage JD
Chief Privacy and Regulatory Officer
Omada Health, Inc.

Attachments

A: Savage, Lucia, et al. *Digital Health Data and Information Sharing: a New Frontier for Healthcare Competition,* 82 ANTITRUST LAW JOURNAL NO. 2 (2019).
B: Comments of Omada Health, Inc. to U. S. Department of Health and Human Services Office for Civil Rights in Response to Request for Information, Docket # 0945AA00, submitted February 10, 2019.
C: Savage, L., *ONC's Proposed Rule On Information Blocking: The Potential To Accelerate Innovation In Health Care,* Health Affairs Blog, February 15, 2019.

DIGITAL HEALTH DATA AND INFORMATION SHARING: A NEW FRONTIER FOR HEALTH CARE COMPETITION?

Lucia Savage
Martin Gaynor
Julia Adler-Milstein*

It has long been the case that information can confer competitive advantage. This has come to be increasingly important, and perhaps central, in many industries as digital interfaces and data storage and processing capacities have grown dramatically. In all sectors of the economy, companies are applying data science to their digital assets to gain insights into the people and behaviors represented in the data. While in many ways health care has lagged in the adoption and effective utilization of information technology,[1] the ability to access and analyze data has become increasingly important in health care, as it has in other sectors of the economy.

Analyzing health data can yield important insights for health care organizations. For example, through data they possess,[2] health care businesses can learn more about the people they are caring for, the practice patterns of their

* Lucia Savage is Chief Privacy and Regulatory Officer at Omada Health, Inc. and is former Chief Privacy Officer at the Office for the National Coordinator for Health IT in the Department of Health and Human Services. Martin Gaynor is the E.J. Barone University Professor of Economics and Health Policy at the Heinz College of Information Systems and Public Policy at Carnegie Mellon University and is former Director of the Bureau of Economics at the Federal Trade Commission. Julia Adler-Milstein is Associate Professor of Medicine and the Director of the Clinical Informatics and Improvement Research Center at the University of California, San Francisco. We thank Nathan Wilson and William Adkinson for helpful comments that substantially improved the article. Responsibility for all views and any errors or omissions are ours alone.

[1] Nikhil Sahni, Robert S. Huckman, Anuraag Chigurupati & David M. Cutler, *The IT Transformation Health Care Needs*, Harv. Bus. Rev., Nov.-Dec. 2017, at 128.

[2] We refer to digital health data via custody rather than ownership because whether anyone besides an individual owns data about them is beyond the scope of this paper. We focus on digital data within the traditional health care system in this paper (also known as digital Protected Health Information under HIPAA). Health data collected in other settings, such as retail or direct-to-consumer services, is outside our scope.

doctors, and the capacity utilization of their facilities. This rich information can be used to assess and improve performance. It has the potential to improve the quality of care and lower costs, benefiting both patients, health care organizations, and the health care system overall. It can be used by individuals to create their own longitudinal health record and monitor their health.[3] In fact, the promise of digital data exchange to improve health underlay Congress' enactment of the Health Information Technology for Clinical Health (HITECH) Act in 2009 as part of the American Recovery and Reinvestment Act,[4] and most recently, the health information technology (IT) provisions of the 21st Century Cures Act in 2016[5] (Cures). Both of these federal laws actively promoted a higher rate of exchange[6] of identifiable health information for all the above reasons.

Yet, even with widespread digitization of health information and a $36 billion-dollar taxpayer investment to make that happen,[7] that information seems to be flowing at a sluggish pace, and the exchange of digital health information among competitors is the exception, not the norm.[8] This is distinct from some other industries where sharing data is more common and firms compete on the basis of using that data to create value.[9]

[3] Ellen M. Harper, *The Economic Value of Health Care Data*, 37 NURSING ADMIN. Q. 105 (2013).

[4] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 et seq. (codified in scattered sections of U.S.C.) [hereinafter ARRA], Title IV, Health Information Technology for Clinical Health Act, [hereinafter HITECH], 123 Stat. 226–79 (2009) (codified in scattered sections of 42 U.S.C.). Certain provisions of ARRA appropriated one-time dollars to stimulate the use of health information technology. Within ARRA, the HITECH §§ 13000–13424, *inter alia*, established the Office of the National Coordinator for Health IT as a full-fledged agency, authorized regulations that specify the technical specifications of certified EHRs, and amended portions of the Health Insurance Portability and Accountability Act and the Privacy, Security and Breach Notification regulations of HIPAA. Health Insurance Portability & Accountability Act, Pub. L. No. 104-191 (1996), 100 Stat. 2548 (codified as amended in scattered sections of U.S.C.) [hereinafter HIPAA].

[5] 21st Century Cures Act, HR 34, Pub. L. No. 114-255, 130 Stat. 1033 (2016) (codified in scattered sections of U.S.C.) [hereinafter Cures].

[6] As used in this article, "exchange" will have two meanings, understood from the context. It means (1) a provider sharing of identifiable health data with another provider for a common patient and (2) the ease with which EHRs enable that sharing.

[7] HITECH & ARRA, *supra* note 4, Title V (money for incentive payments to physicians and hospitals who "meaningfully used" certified electronic health records). R

[8] The Federal Trade Commission explored competition and information exchange in a 2014 workshop. *See generally* Fed. Trade Comm'n, Examining Health Care Competition (Mar. 20–21, 2014), www.ftc.gov/news-events/events-calendar/2014/03/examining-health-care-competition.

[9] Extensive information exchange between rivals occurs in some other industries (but not all). Financial institutions fiercely compete for customer business and regularly exchange information from their customers' accounts. Cellular phone customers can change carriers and equipment without the carrier refusing to exchange or transfer the data (although a federal law was required to make this easier for the consumer). In on-line search, customers can easily transfer their bookmarks, settings, and search histories across browsers, although search engines retain proprietary custody of the search histories they collect. Online shopping sites typically retain their custom-

In this article, we argue that the sluggish pace of information exchange results from firms' incentives and abilities to maintain or enhance their competitive advantage. Health care organizations and their software vendors control the data collected or generated in the course of patients' encounters with them. These organizations decide if, when, and how they will share that information with others, including other health care organizations, other software vendors, and, in some cases, even the patients themselves.[10]

Not surprisingly, if retaining data is profitable while sharing it is not, there will not be a large amount of data sharing. In particular, if firms perceive that control of these data confer competitive advantage, they will be reluctant to share the data with rivals, even if sharing the data likely enables better care to be delivered to patients. Holding on to data may allow market participants to maintain, and in some cases enhance, their market position.[11] We believe this "data blocking" is already a barrier to choice and competition and can make it difficult for new innovative organizations to successfully enter health care markets and compete. Furthermore, we anticipate that these issues will become even more pressing as data become an ever more important asset in health care, as it is in the rest of the economy.

The Executive and Legislative branches have recognized the apparent lack of data sharing by health care organizations may be attributable to data blocking (also called "information blocking"). In 2014, Congress requested that the U.S. Department of Health and Human Services Office of the National Coordinator for Health IT (ONC) publish a report on information blocking.[12] Information blocking occurs when an entity that controls health data—such as a

ers' data and do not share. Control of data and what that means for competition has become a major issue in high-tech industries. *See, e.g.*, OECD, Big Data: Bringing Competition Policy to the Digital Era (Oct. 27, 2016), one.oecd.org/wdocument/DAF/COMP(2016)14/en/pdf (background note by the Secretariat).

[10] While HIPAA, *supra* note 4, requires that providers give patients their Protected Health Information (PHI) when it is requested, patient complaints about inability to get their own data remains the number one type of complaint to OCR. U.S. Dep't of Health & Human Servs., Office for Civil Rights, *Top Five Issues Investigated* (Jan. 31, 2018), www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html. R

[11] Joy Grossman, Kathryn Kushner & Elizabeth November, *Creating Sustainable Local Health Information Exchanges: Can Barriers to Stakeholder Participation Be Overcome?* Research Brief, Center for Studying Health System Change (2008), www.hschange.org/CONTENT/970/970.pdf. This study conducted interviews with health care stakeholders in four communities regarding the sharing of health data and found that hospitals "viewed clinical data as a key strategic asset, tying physicians and patients to their organization." *Id.* at 5.

[12] Consolidated and Further Continuing Appropriations Act 2015, Pub. L. No. 113-235, 128 Stat. 2138 (codified in scattered sections of U.S.C.). *See also* 160 Cong. Rec. H9047, H9839 (daily ed. Dec. 11, 2014) (explanatory statement submitted by Rep. Rogers, Chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015) (2015 Budget Act).

health care organization or an electronic health record (EHR)[13] software vendor—refuses to share the data or engages in practices that impede efficient access and use of the data by competitors or other individuals or entities.

In April 2015, ONC published the report requested by Congress on the nature and extent of information blocking.[14] In late 2016, Congress passed the 21st Century Cures Act (Cures).[15] Cures defines information blocking, and requires ONC in conjunction with the HHS Office of the Inspector General (OIG) to define business practices that do not constitute information blocking.[16] It also authorizes OIG to root out information blocking, including authorizing levying fines of up to $1 million per violation.[17] On February 11, 2019, ONC released an "HHS approved" draft of its Notice of Proposed Rulemaking to Improve the Interoperability of Health Information, which will be published shortly in the Federal Register.[18]

Whether these provisions will be sufficiently strong to overcome firms' incentives to engage in information blocking remains an open question. In what follows, we trace the background and public policy behind the federal government's drive to dramatically increase the availability of clinical digital health data and its expectation that those data would be exchanged widely and appropriately.[19] We focus on how the sharing (and lack of sharing) of clinical

[13] HITECH subtitle A, part I, § 13001(1), defines Electronic Health Records statutorily. CMS (Centers for Medicare and Medicaid Services) offers a layperson's definition as

> an electronic version of a patient's medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person's care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.

U.S. Ctrs. for Medicare & Medicaid Servs., U.S. Dep't of Health & Human Servs., Electronic Health Records (Mar. 26, 2012), www.cms.gov/Medicare/E-Health/EHealthRecords/index.html. Regulations promulgated by the Office of the National Coordinator for Health IT (ONC) (codified at 45 C.F.R. § 170.300 et seq.) specify the functions an EHR must meet to be "certified." As is discussed, *infra* note 33, to be eligible to receive financial incentives from CMS, physicians **R** and hospitals must use EHRs that are certified.

[14] OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., U.S. DEP'T OF HEALTH & HUMAN SERVS., REPORT ON HEALTH INFORMATION BLOCKING (Apr. 2015) [hereinafter ONC INFORMATION BLOCKING REPORT], www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.

[15] Cures, *supra* note 5, Title IV, §§ 4001–4006. **R**

[16] *Id.* 130 Stat. 1177 (codified at 42 U.S.C. 300jj–52(a)(2)(C)).

[17] *Id.* § 4004 (creating § 3022(b) of the Public Health Service Act, 42 U.S.C. § 300jj-52(b)).

[18] 84 Fed. Reg. 7424 (Mar. 4, 2019), ONC *Notice of Proposed Rulemaking to Improve the Interoperability of Health Information* (Feb. 11, 2019), www.healthit.gov/topic/laws-regulation-and-policy/notice-proposed-rulemaking-improve-interoperability-health. ONC's Notice of Proposed Rule Making is consistent with our analysis below because the proposed rule prohibits "information blocking" as defined, unless one of seven exceptions apply, but only when the activity is not anticompetitive, per a proposed 45 C.F.R. 170.404(a)(3)(i)(B)(4).

[19] We focus on clinical digital health data from a care setting, as opposed to administrative digital health data, because the former has been the focus of HITECH and subsequent federal

digital health data affects competition. We analyze the problem from the perspectives of the health care providers and EHR vendors, the most important participants in the flow of patient medical data from an antitrust and policy perspective. We conclude with a look forward and suggestions of policy efforts that could shift firms' incentives from not sharing data to sharing it.

I. FEDERAL POLICY TO DIGITIZE HEALTH INFORMATION AND PROMOTE INFORMATION SHARING

In this Part, we first briefly describe the federal legal landscape that permits physicians and hospitals to exchange identifiable health information about patients they have in common. Next, we summarize how Congress built on that foundation in 2009 by enacting HITECH, creating significant financial incentives for physicians and hospitals to digitize their record keeping and to share the resulting digital data.

A. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SUPPORTS INFORMATION SHARING

In 1996, Congress passed the Health Information Portability and Accountability Act (HIPAA).[20] Although this act is now synonymous with the health information privacy regulation it spawned, HIPAA actually focused on two other features. "Portability" refers to insurance coverage portability, not data portability. (Twenty years ago policy makers believed insurance coverage portability would help alleviate the worse health effects of pre-existing condition exclusions to insurance coverage.) "Accountability" referred to the federal legal requirement that, in order to be paid by CMS (Centers for Medicare and Medicaid Services), providers would have to bill CMS digitally and therefore digitize claims information. Thus, through HIPAA, Congress made its first attempt to bring the power of computing to health care, specifically in the context of data transmissions. To avoid unintended consequences deriving from the electronic billing requirement, Congress delegated to HHS the development of regulations that specified how digital health data can be accessed, used and disclosed.[21] As a result, we have the HIPAA Privacy, Security and Breach Notification federal regulations still in use today.[22] In general, unless

policy. While the sharing of claims data between payers and providers is an important topic, which is also subject to incentives and market forces, payers were not directly affected by the provisions of HITECH.

[20] HIPAA, *supra* note 4.

[21] Daniel J. Solove, *HIPAA Turns 10: Analyzing the Past, Present and Future Impact*, 84 J. AHIMA 22 (2013).

[22] Although 45 C.F.R. §§ 160–164 state all of the Privacy, Security and Breach Notification Rules, most of the Privacy Rule is found at 45 C.F.R. §§ 164.500–164.536, most of the Security Rule is found at 45 C.F.R. §§ 164.300–164.318, and most of the Breach Notification Rule, not relevant for the present discussion, is found at 45 C.F.R. §§ 400–414.

the context requires more specificity, we will simply refer to HIPAA for the totality of the Privacy, Security, and Breach Notification rules.

What HIPAA permits and requires by way of information sharing is important, because if HIPAA does not permit sharing, holders of data protected by HIPAA should not be accused of "information blocking." But, where HIPAA permits or even requires data sharing, a failure to do so should be examined to make sure that HIPAA is not being employed as a pretext to justify data "hoarding," as has been alleged by ONC,[23] or to prevent patients from being "poached."[24] Therefore, we will briefly summarize what HIPAA permits and requires relative to information sharing.

The basic regulations governing when health information protected by HIPAA can be exchanged were written in 2000 and 2002, and are unchanged since then.[25] HIPAA applies to the holders of identifiable health information, called "protected health information" or PHI, when those holders (called "covered entities") are physicians, hospitals, health plans (including self-funded employer medical benefits plans), and certain businesses that process digital health information for billing. We are focused on health information in the custody of physicians and hospitals. HIPAA further recognizes that covered entities will need to hire various "business associates" to serve special purposes. The Privacy and Security Rules apply to both covered entities and business associates either by regulation or contract. For hospitals and physicians, EHR vendors are their business associates under HIPAA.[26]

HIPAA requires that when requested to do so, covered entities provide an individual with copies of that individual's PHI. The individual can then do whatever he or she wants with it, including giving it to another covered en-

[23] Genevieve Morris, Principal Deputy Nat'l Coordinator for Health IT, Panelist at Annual Meeting of the Office of the Nat'l Coordinator for Health IT, at 27:16 (Nov. 30, 2017), events.tvworldwide.com/Events/ONCAnnualMeeting2017_Breakout/VideoId/-1/UseHtml5/True.

[24] Seema Verma, Admin'r, Ctrs. for Medicare & Medicaid Servs., Remarks by Administrator Seema Verma at the ONC Interoperability Forum (Aug. 6, 2018), www.cms.gov/newsroom/press-releases/speech-remarks-administrator-seema-verma-onc-interoperability-forum-washington-dc.

[25] Office of the Nat'l Coordinator for Health Info. Tech. & HHS Office for Civil Rights Fact Sheets on exchange for treatment and exchange for health care operations of the recipient, published in 2016, describe and illustrate 45 C.F.R. §§ 164.501, 164.506, and some provisions of § 164.512. Office of the Nat'l Coordinator for Health Info. Tech., *Fact Sheets* [hereinafter *HIPAA Fact Sheets*], www.healthit.gov/topic/fact-sheets. In essence, as between two traditional health care organizations, like hospitals and physicians, the fact sheets show that exchange for treatment is *permitted* without first obtaining an individual's written permission, but not *required.* In contrast, when an individual asks for a copy of his or her own health information, including electronically via a download or transmit function on an EHR, release of the data is *required. See, e.g.*, 45 C.F.R. § 164.524. Thus, no federal regulations require physicians or hospitals to exchange health information with each other.

[26] *See* 45 C.F.R. § 164.504 (2000, amended 2013).

tity.[27] In HITECH, Congress interpreted this regulation, and required that where a person sought his or her PHI from a health care organization that used a certified EHR, the person must be able to view, download, or transmit their PHI to a recipient of his or her's own choosing,[28] including a competing provider. HIPAA also permits two covered entities to share PHI, without the person's written consent, about a person to whom they are both delivering care.[29] In 2015, the HHS Office for Civil Rights clarified that this permission includes sharing health information using ONC certified EHRs.[30] That guidance also specified that the disclosing covered entity was legally not responsible for the security conditions at the recipient covered entity. As a result, it is well documented that while other privacy rules may place additional restrictions on when and how sharing occurs, lack of health information sharing is not due to HIPAA specifically prohibiting it.[31]

B. HITECH Incentivizes Information Sharing

HITECH,[32] passed in 2009, provided over $36 billion in incentive payments for physicians and hospitals to adopt and meaningfully use (as specified by CMS "Meaningful Use" criteria)[33] software (with functions prescribed by ONC)[34] to keep track of their patients' medical care through EHRs. HITECH provided further incentives for digitizing health records, this time clinical, not claims, data. Under HITECH, a physician or hospital that adopted a certified electronic health record that met minimum software specifications, and which used that software as specified by CMS Meaningful Use criteria, was eligible for significant payments—$44,000 per physician for full Stage 1 compliance.[35] The incentive payments were intended to compensate providers for the acquisition costs of the EHRs.[36]

[27] 45 C.F.R. § 164.524 (2000, amended 2013).

[28] HITECH, *supra* note 4, § 13405(e). R

[29] 45 C.F.R. § 164.506(c)(2) & (c)(4).

[30] *HIPAA Fact Sheets*, *supra* note 25. R

[31] Michelle Mello, Julia Adler-Milstein, Lucia Savage & Karen Ding, *Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles?*, 96 MILBANK Q. 110 (Mar. 2018) [hereinafter Mello et al., *Boulders or Pebbles*].

[32] Pub. L No. 111–5, 123 Stat. 226 (2009) (codified in scattered sections of U.S.C.).

[33] *See* HITECH, *supra* note 4, §§ 4101–4102; 42 C.F.R. §§ 412, 413, 422 & 495. This method—payment incentives for new behaviors it wants—now infuses many other CMS payment rules, such as the Medicare Inpatient Prospective Payment Rule for Hospitals and the Medicare Physician Fee Schedule for physicians. For example, see generally 2019 Medicare Inpatient Prospective Payment, 83 Fed. Reg. 41,144, 41,634–88 (Aug. 17, 2018). R

[34] HITECH, *supra* note 4, § 3001; 42 C.F.R. § 170.300 et seq. (regulations). R

[35] Ctrs. for Medicare & Medicaid Servs., Dep't of Health & Human Services, *An Introduction to the Medicare Meaningful Use Program for Eligible Professionals*, slide 12 (undated), www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/beginners_guide.pdf.

[36] HITECH, *supra* note 4, §§ 4101–4102. R

This whole scheme was called "Meaningful Use" or "the Meaningful Use Program," after language in HITECH.[37] Meaningful Use had three stages.[38] The criteria required to qualify for meaningful use payments became more demanding at each successive stage. For example, in Stage I physicians and hospitals had to attest to a criterion that required having received health information from someone else.[39] In Stage II, they had to attest to a criterion that required having sent it somewhere else, and to having allowed patients who wanted it the ability to download or transmit their own health information directly from the relevant EHR.[40]

ARRA also made $300 million available for seed money grants (to be awarded by ONC) to states or organizations designated by states, to build technical and governance infrastructure to enable physicians and hospitals to share information with each other.[41] There were also funds available to Medicaid agencies within states to build connectivity and ensure that Medicaid beneficiaries also got the clinical and efficiency benefits of health information exchange.[42] Even after the official "Meaningful Use" program began to end, CMS continues to use this method to change provider behaviors in general, and in particular about information sharing.[43]

By the end of 2016, most of the $36 billion had flowed to EHR vendors.[44] According to ONC, more than 95 percent of acute care hospitals and 78 percent of physicians were "meaningfully using" electronic health records, as a

[37] *Id.*

[38] Medicare & Medicaid Programs; Electronic Health Record Incentive Program, 75 Fed. Reg. 44,313 (July 28, 2010).

[39] Final Stage 1 regulations were effective in 2011 and superseded by subsequent regulations, all of which updated 42 C.F.R. § 170.300 et seq.

[40] 42 C.F.R. § 412 (for hospitals); 42 C.F.R. § 495 (for physicians). We note that with each year's new measurement and incentive payment regulations, the regulatory nomenclature and incentive requirements change. For example, for calendar year 2019, what used to be called meaningful use for hospital is now called "promoting interoperability," 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 41,144, 41,635 (Aug. 17, 2018).

[41] ARRA, *supra* note 4, Sec. 5, Div. A, Title I, ONC Appropriation, 123 Stat. 179 (2009). R

[42] Letter from Vikki Wachino, Dir., Ctrs. for Medicare & Medicaid Services, Dep't of Health & Human Services, to State Medicaid Directors (Feb. 29, 2016), www.medicaid.gov/federal-policy-guidance/downloads/smd16003.pdf.

[43] For example, the 2019 Medicare Inpatient Prospective Payment Rule still financially rewards hospitals which can attest to exchange for a single patient. 83 Fed. Reg. 41,144 (Aug. 7, 2018). As for financial penalties, the proposed 2019 Inpatient Payment Rule requested information on whether a failure to meet certain health sharing behaviors could lead to a hospital not being allowed to participate in the Medicare program at all. 83 Fed. Reg. 20,164, 20,550 (May 7, 2018). However, in the 2019 Medicare Inpatient Prospective Payment Rule, Medicare did not impose this type of penalty. 83 Fed. Reg. 41,144, 41,688 (Aug. 17, 2018).

[44] Joseph Conn, *Epic, Cerner EHRs Top the List for Hospital Meaningful-Use Payments*, MODERN HEALTHCARE (May 12, 2014), www.modernhealthcare.com/article/20140502/NEWS/305029944.

result of HITECH and its incentives.[45] This means that the vast majority of Americans have some, and possibly a lot, of their health data stored in digital form.

Although the volume of digital clinical health data grew substantially, data were not being exchanged. Many hospitals and providers met the Meaningful Use criterion that required electronic transmission of a summary of care record for at least 10 percent of transitions from provider to provider or one care setting to another (as part of meeting the second stage of Meaningful Use requirements).[46] Few of them, however, did so for the majority of care transitions.[47] National hospital data from 2014 reveal that only 25 percent of hospitals routinely engaged in four dimensions of interoperability—finding, sending, receiving, and integrating data from outside providers.[48] One year later, this had only increased to 30 percent, suggesting a slow transition to nationwide interoperability.[49]

In parallel with national data revealing slow progress on interoperability, anecdotal reports of information blocking emerged.[50] Lawmakers and other stakeholders became concerned that the slow progress on interoperability was, at least in part, driven by information blocking behaviors. In response, Congress requested that ONC investigate.[51]

The resulting report[52] summarized available evidence of information blocking and included examples of these practices, including unreasonably high fees for technical connections, pretextual use of privacy laws as a justification for not sharing information, and various contractual and other business practices that limit the exchange of information with competitors. The agency con-

[45] OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., OFFICE OF THE SEC'Y, U.S. DEP'T OF HEALTH & HUMAN SERVS., 2016 REPORT TO CONGRESS ON HEALTH IT PROGRESS: EXAMINING THE HITECH ERA AND THE FUTURE OF HEALTH IT SUBMITTED PURSUANT TO SECTION 3001(C)(6) OF THE PUBLIC HEALTH SERVICE ACT AND SECTION 13113(A) OF THE HITECH ACT (2016) at 5.

[46] CMS Electronic Health Record Stage 2 Final Rule, 79 Fed. Reg. 52,909 (Sept. 4, 2014).

[47] Sunny C. Lin, Jordan Everson & Julia Adler-Milstein, *Technology, Incentives, or Both? Factors Related to Level of Hospital Health Information Exchange*, 53 J. HEALTH SERVS. RES. 3278 (2018).

[48] A Jay Holmgren, Vaishali Patel & Julia Adler-Milstein. *Progress in Interoperability: Measuring US Hospitals' Engagement in Sharing Patient Data*, 36 HEALTH AFF. 1820, 1820 (2017).

[49] *Id.* at 1825

[50] This is summarized in Nick Terry, *Information Blocking and Interoperability*, BILL OF HEALTH (Dec. 19, 2014), blogs.harvard.edu/billofhealth/2014/12/19/information-blocking-and-interoperability/.

[51] 2015 Budget Act, *supra* note 12, 128 Stat. 2483–484. *See also* 160 CONG. REC. H9839 (daily ed. Dec. 11, 2014) (explanatory statement submitted by Rep. Rogers, chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015). **R**

[52] ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 17. **R**

cluded both that information blocking was occurring and that it was a serious impediment to the appropriate flow of health information.[53]

Further, the ONC Information Blocking Report expressed concern that one aspect of information blocking represented potentially anticompetitive conduct. EHR developers and health care providers were not exchanging health information outside their closed systems. ONC's concern was that this failure to exchange information sometimes reflected deliberate attempts to disadvantage rivals by withholding information.[54]

From a legal perspective, providers and hospitals received substantial financial payments for legally attesting to having undertaken certain activities, including a specific, albeit minimal level of exchange.[55] If the attestations were proved false, they would be subject to the same rules as any other false or fraudulent claim to CMS.[56] However, the second, and more likely, scenario was a set of activities that were not false attestations. For example, the amount of activity required to meet the incentive milestone was sometimes quite low, such as a single occurrence of information exchange with an unaffiliated provider in a 12-month period. In practice, providers and hospitals could both legally attest to the minimal quantity amounts of exchange and still engage in information blocking beyond those minimums.

We do not know whether CMS and ONC were "naïve"[57] regarding the prospect that organizations would meet the requirements while still engaging in information blocking, or realized the possibility but did not think it would be widespread. By the time it wrote the Information Blocking Report, however, ONC clarified that HITECH was enacted with the goal of spurring data-driven competition among health care delivery organizations.[58]

As mentioned earlier, following ONC's February 2015 report, Congress responded in 2016 by enacting the 21st Century Cures Act,[59] outlawing information blocking, except as required by law or specified in future

[53] *See, e.g.*, *id.* at 16.

[54] *Id.* at 15.

[55] *See, e.g.*, *id.* at 4, 17.

[56] Press Release, U.S. Dept. of Justice, Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations (May 31, 2017), www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.

[57] Sarah Kliff, *The Fax of Life: Why American Medicine Still Runs on Fax Machines*, VOX (Jan. 12, 2018), www.vox.com/health-care/2017/10/30/16228054/american-medical-system-fax-machines-why.

[58] Promoting "a more effective marketplace, greater competition . . . increased consumer choice, and improved outcomes in health care services" is one of the express purposes of a nationwide health IT infrastructure for health information exchange. ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 10. *See also* Public Health Service Act § 3001(b)(10), 42 U.S.C. § 300jj–11(b)(10). R

[59] Cures, *supra* note 5, §§ 4001–4006 (codified in scattered sections of 42 U.S.C.).

rulemaking.[60] It also directed the HHS Office of the Inspector General and ONC to collectively develop standards via rulemaking for recognizing unlawful information blocking.[61]

Meanwhile, there was an effort to examine the extent of information blocking by surveying leaders of digital health data exchange efforts across the country. The survey revealed that 60 percent of respondents reported that hospitals and health systems routinely or occasionally engage in information blocking, while 85 percent of respondents reported that EHR vendors do so.[62] The survey also identified common forms of information blocking pursued by providers (e.g., controlling patient flow by selectively sharing data) and by EHR vendors (e.g., charging fees for sharing that were unrelated to actual cost to provide sharing capabilities).[63] While not all health care stakeholders are convinced that information blocking is real,[64] prominent stakeholders, including the American Medical Association, American Academy of Family Practitioners, and Health IT Now continue to advocate to ONC and OIG on whether information blocking is a significant problem and, if so, how it should be defined.[65] Recently, Principal Deputy National Coordinator Genevieve Morris declared, "We have to stop competing on hoarding data"[66] And Medicare Administrator Seema Verma stated that hospital "[s]ystems too often refuse to share data because they fear their patients will be poached. This mentality has to be changed because it endangers the health of millions of Americans.[67]

As the preceding demonstrates, federal law requires or permits information sharing, and Congress has gone to great and repeated lengths to promote shar-

[60] *Id.* § 4004 (codified at 42 U.S.C. § 300-jj-52(a)(1)).

[61] *Id.* § 4006(a)(3), 130 Stat. 1177 (codified at 42 U.S.C. § 300jj-52(a)(3)) ("The Secretary, through rulemaking, shall identify reasonable and necessary activities that do not information blocking for purposes of paragraph.").

[62] Julia Adler-Milstein & Eric Pfeifer, *Information Blocking: Is It Occurring and What Policy Strategies Can Address It?*, 95 MILBANK Q. 117 (2017).

[63] ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 15. R

[64] *Dr. John Halamka: 4 Thoughts on MU, Information Blocking and Interoperability,* BECKER'S HOSP. REV. (June 02, 2015), www.healthleadersmedia.com/innovation/countdown-information-blocking-rule-progress (quoting John Halamka, MD, CIO of Harvard-affiliated Beth Israel Deaconess Medical Center in Boston, "I've never seen it. Find me one example"); Mandy Roth, *Countdown to Information Blocking Rule in Progress*, HEALTH LEADERS MEDIA (Sept. 28, 2018), www.healthleadersmedia.com/innovation/countdown-information-blocking-rule-progress (quoting Marc Probst, CIO of Intermountain Health Care in Utah, "Data blocking is a bit like a mythical creature. . . . I think they [HHS] are stretching it a bit when they talk about some of the things that have happened around data blocking.").

[65] Press Release, Health IT Now, *Health IT Now Sends Information Blocking Recommendations to ONC, HHS and OIG* (Aug. 29, 2017), www.healthitnow.org/press-releases/2017/8/29/health-it-now-sends-information-blocking-recommendations-to-onc-hhs-oig (reporting that a group of organizations, including IBM and the American Academy of Family Physicians, sent recommendations for addressing information blocking to ONC).

[66] Morris, *supra* note 23, at 27:16. R

[67] Verma, *supra* note 24. R

ing. Yet, exchange is not occurring at the rates hoped for, or even anticipated. Therefore, this prompts us to consider what else may be driving or contributing to the low rates of exchange. Below, we examine all the justifications that have been reasonably asserted and conclude that anticompetitive motivations may be suppressing the rate of health information exchange, despite a clear public policy favoring it. In Part IV, we suggest additional actions that could be undertaken to better understand why rates of health information exchange remain so low and potentially to help remedy the problem.

II. FACTORS AFFECTING INFORMATION SHARING

In what follows we consider legal or technical factors that may impede data sharing among health care organizations, then explain how these factors (privacy, security, technical challenges, etc.) relate to different health care organizations' financial incentives. We conclude that these firms too often make it harder than it needs to be (legally or technically) for patients to take their data to other firms because this can inhibit patients or customers from moving their business to competing providers. This conduct thwarts federal policy goals of increasing consumer choice and competition in health care.

A. JUSTIFICATIONS FOR NOT SHARING HEALTH INFORMATION

Health care systems and providers, as well as EHR vendors, have offered various justifications for not exchanging health information. These include patient privacy, ensuring proper security of health information, intellectual property, and the costs and complexity of software interfaces. While some of these are legitimate (at least in certain circumstances), some do not hold up legally or factually. We discuss each of these below. For example, health care providers have claimed that HIPAA regulations are a reason why information cannot be shared. However, as we demonstrated above, this nationwide health privacy law actually has more than a dozen reasons why sharing health information among providers is permitted or even required.[68] In addition, while there are some technical challenges associated with sharing digital health data, experts believe these technical barriers can be overcome, as they have been in other industries.[69]

[68] *See, e.g.*, 45 C.F.R. § 164.506(c) (listing some reasons why disclosure is permitted); C.F.R. § 164.524 (stating disclosures required to an individual of their own health information).

[69] ONC API TASK FORCE RECOMMENDATIONS (May 12, 2016) [hereinafter ONC API TASK FORCE], www.healthit.gov/sites/default/files/facas/HITJC_APITF_Recommendations.pdf; *see also* ESAC INC. & SRS, INC., KEY PRIVACY AND SECURITY CONSIDERATIONS FOR HEALTH CARE APPLICATION PROGRAMMING INTERFACES (APIS) (Dec. 2017) (Contract: HHSP23320160022 4A), www.healthit.gov/sites/default/files/privacy-security-api.pdf; ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 8; Mello et al., *Boulders or Pebbles*, *supra* note 31. R

In what follows, we first discuss factors affecting information sharing by EHR developers, then health care providers. We analyze their financial incentives regarding information sharing, and legal or technical barriers to doing so.

B. FINANCIAL INCENTIVES AFFECTING EHR DEVELOPERS' INFORMATION SHARING

As discussed above, Congress provided significant financial incentives through the Meaningful Use program to make health information exchange more widespread, and the basic federal health information law permits the contemplated exchange without the written permission of the individual.[70] Despite this, there is still little exchange of data. In order to understand this, one must examine how firms' overall economic interests are affected by data exchange. At present no business model exists for EHR companies to profit from data sharing. In fact, holders of PHI are not allowed to sell it,[71] and for permitted disclosures (discussed in Part I.A above), PHI holders are allowed to recover only their "reasonable" costs for preparing and transmitting data.[72] On the other hand, EHR companies may have substantial financial incentives to retain data and avoid facilitating their physician and hospital customers from sharing the health information outside of business relationships the EHR company controls.

While the financial incentives at play for any given vendor depend on its business model, and precise information on the business models used is not publicly available, there is a common understanding of how different business models create competitive benefit from not sharing data.[73] The first and most direct incentive is the way vendors are paid. An EHR company that is paid based on the number of individuals whose records they process has strong incentives to retain the data and strong disincentives to make it easy for an individual to move their data to a competing provider. When patient data migrate from one vendor to another, the source vendor directly loses revenue, which is gained by competitors.

A second financial incentive to retain data is that the data held by an EHR company can be exploited for analytics. The greater the volume of data a firm

[70] 45 C.F.R. 164.506(c).

[71] 45 C.F.R. 164.502(a)(5)(viii) (interpreting HITECH, *supra* note 4, § 13406 (codified at 42 U.S.C. 17936 (2009))). R

[72] 45 C.F.R. 154.502(a)(5)(ii) & (viii).

[73] Jordan Everson & Julia Adler-Milstein, *Engagement in Hospital Health Information Exchange Is Associated with Vendor Marketplace Dominance*, 35 HEALTH AFF. 1286 (2016) (finding that there is more information exchange in markets where the dominant EHR vendor has a smaller market share, suggesting that competition and information exchange may be positively related).

holds, the more informative, and hence valuable, the analytics it can produce are for customers, who may use them for research, clinical decision support, business decision support, etc.[74] An NIH blog suggests that EHR data may be "the most high-value data set to come."[75] For example, this year, Flatiron Health, a privately held oncology EHR company, sold for $1.9 billion because of the value of its data.[76]

A third financial incentive affecting information sharing is that lack of interoperability between EHRs can financially benefit the EHR companies. If an EHR is more valuable to any user the more it is adopted by other users, then EHR companies have a strong incentive to build and retain market share to become the dominant EHR.[77] This is because if an EHR has more patients, it has more data for analysis, an attractive feature for prospective providers.[78] The EHR vendor is thus likely to become a "must have" data destination. Interoperability undermines that value, enabling providers to acquire patient records outside that particular vendor and its closed environment.

In its Information Blocking Report, ONC discussed the rise of these "walled gardens," technical environments in which every provider who contracts with that EHR developer may be able to exchange with other customers of that vendor, but not outside the "garden walls."[79] A dominant vendor has the most data on the most patients within the referral market, and on the most physicians in the referral market. This dominant position creates pressure for providers not using the dominant vendor to switch because that is where the patient data are. While, of course, there may be interoperability *within* one EHR developer's data system used by many providers, effective competition among EHR developers and the innovation and downward price pressure it brings, languishes.

[74] An example is Flatiron Health, which developed and hosts data for an oncology-only EHR, with the express business model of aggregating data sets to improve cancer research, better clinical decision support, etc. Christina Farr, *At Flatiron Health, Keeping the Doctor Close,* FAST COMPANY (Apr. 19, 2017), www.fastcompany.com/3067893/at-flatiron-health-keeping-the-doctor-close.

[75] Patti Brennan, *Is the EHR the New Big Data?*, NAT'L INST. OF HEALTH, DataScience@NIH, (Mar. 24, 2017), datascience.nih.gov/BlogIsTheEHR.

[76] Sy Mukherjee, *Why Drug Giant Roche's $1.9 Billion Deal to Buy Data Startup Flatiron Health Matters*, FORTUNE (Feb. 16, 2018), fortune.com/2018/02/16/roche-flatiron-health-deal-why-it-matters/.

[77] This phenomenon is referred to as a "network externality." A product or service is more valuable the more other people adopt or use it. This phenomenon is familiar from computer operating systems and software, microprocessors, telecommunications, and electronic marketplaces.

[78] Depending on the EHR developer's business model, greater numbers of patient records may also mean greater revenue.

[79] ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 17–18. R

A fourth form of financial incentive is that EHR developers can and do charge providers high fees for connectivity to other vendor systems or with third parties, such as fees that a developer charges to engineer software to connect securely to another vendor's software. These make interoperability, and thus data sharing, expensive, but improve the developer's bottom line. Of course, fees at some level may be reasonable, but providers (especially small practices, which constitute the majority of providers outside of hospitals)[80] argue that the fees are disproportionately high compared to the technological challenge, do not account for economies of scale, and in fact are priced high to discourage connectivity and exchange.[81] Thus, the fees can serve as financial barriers for physicians who want to exchange data with providers who use competing EHR systems, and confine those physicians to the aforementioned "walled gardens." Thus, charging high fees can be a strategy for data holders to impede data transfer and thwart competition. This may be a version of the strategy of raising rivals' costs to thwart competition.[82]

Developers, however, argue that they need to restrict information sharing to protect the intellectual property underlying their systems. In particular, there is concern that making information available for sharing could reveal two business sensitive sources of IP: (1) their underlying data model (i.e., how information is stored and organized), and (2) how the data are presented (i.e., aspects of their user interface). For example, Cerner's terms of use prohibit the Los Angeles County Department of Health Services from disclosing "source code, prices, trade secrets, mask works, databases, designs and techniques, models, displays and manuals."[83]

When source code cannot be disclosed, competing EHR developers, or physicians who hire their own software engineers, cannot develop the tools to

[80] According to the AMA, in 2015 more than 60% of physicians provide care in practices of 10 or fewer physicians. *See* Press Release, Am. Med. Ass'n, AMA Study Finds Majority of Physicians Still Work in Small Practices (July 8, 2015), www.ama-assn.org/content/new-ama-study-reveals-majority-americas-physicians-still-work-small-practices.

[81] ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 15–17. *America's Health IT Transformation: Translating the Promise of Electronic Health Records into Better Care: Hearing Before the S. Comm.*, 114th Cong. 114-578 (Mar. 17, 2015), 161 CONG. REC. D279 (Mar. 17, 2015); *Achieving the Promise of Health Information Technology: Information Blocking and Potential Solutions*, *Hearing Before S. Comm. on Health, Education, Labor and Pension*, 114th Cong. 670 (July 23, 2015), 161 CONG. REC. D870 (daily ed. July 23, 2015); *Achieving the Promise of Health Information Technology*, *Hearing Before S. Comm. on Health, Education, Labor and Pension*, 161 CONG. REC. D870 (daily ed. Oct. 1, 2015) [collectively, *Senate Information Blocking Hearings*], www.help.senate.gov/hearings/achieving-the-promise-of-health-information-technology. R

[82] Steven C. Salop & David T. Scheffman, *Raising Rivals' Costs*, 73 AM. ECON. REV. 267 (1983).

[83] Darius Tahir, *Doctors Barred from Discussing Safety Glitches in U.S.-Funded Software*, POLITICO (Sept. 11, 2015), www.politico.com/story/2015/09/doctors-barred-from-discussing-safety-glitches-in-us-funded-software-213553.

engineer appropriate data connections between two vendors' systems, even if this is what the providers want for patient care. The legitimacy of intellectual property must be recognized and protected, but as in other areas of IT,[84] developers need to make key information available to others who are engineering connections or applications to the platform.[85]

In fact, creating open specifications, available to third-party developers, was a key goal of the API provisions of ONCs 2015 rule.[86] How EHR developers are responding is mixed. On the one hand, they seem to be listening: as of June 2018, 159 developers of certified EHRs have proven to ONC that they have shipped this update to their customers, even if their customers, the providers and hospitals,[87] are not required to make it available until January 2019.[88] But according to Aneesh Chopra, former Chief Technology Officer for the United States, only a handful of hospitals have actually turned on this functionality.[89] There is also public concern that despite including the API technology, the two largest EHR developers are charging high fees for third-

[84] *See, e.g.*, Decision & Order, Intel, FTC Docket No. 9341 (Oct. 29, 2010), www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter; MSC.Software Corp., FTC Docket No. 9299 (June 10, 2003), www.ftc.gov/enforcement/cases-proceedings/0010077/mscsoftware-corporation; Silicon Graphics, 60 Fed. Reg. 35,032 (July 5, 1995); Press Release, Fed. Trade Comm'n, Silicon Graphics, Inc. (June 9, 1995), www.ftc.gov/news-events/press-releases/1995/06/silicon-graphics-inc.

[85] In its rule on Certified EHRs, ONC required for the first time that developers add to the next version an "open specification, read-only" application programming interface, such as is commonly used for financial data already. *See* 45 C.F.R. § 170.315(g)(7), (8) & (9); 2015 Ed. Health Information Technology (Health IT) Certification Criteria, 80 Fed. Reg. 62,602 (Oct. 16, 2015) [hereinafter 2015 Health IT Cert Criteria]. CMS then required in its payment rules under the Medicare Access and CHIP Reauthorization Act of 2015, Pub. L. No. 114–10, 129 Stat. 87 (codified in scattered sections of 42 U.S.C.), that physicians seeking incentive payments allow developers to use those open specifications to develop third-party apps, which individuals would use to get copies of their own health information, called "consumer mediated exchange," or a B2C transaction. Medicare 2018 Updates to the Quality Payment Program, 82 Fed. Reg. 77,008 (Nov. 1, 2016). CMS repeated this requirement for hospitals in its 2018 Medicare Inpatient Prospective Payment Rule, 82 Fed. Reg. 53,568 (Nov. 16, 2017), and reiterated that effective date in the 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 41,144, 41,635–36 (Aug. 17, 2018). It remains to be seen if requiring this change in the software functionality will facilitate greater amounts of business-to-business/provider-to-provider exchange.

[86] 2015 Health IT Cert Criteria, *supra* note 85, 80 Fed. Reg. 62,602, 62,675–76 (Oct. 16, 2015) (noting that how organizations implement the required API should not "block" information sharing by API). R

[87] ONC CERTIFIED HEALTH IT PRODUCTS LIST, CHPL.HEALTHIT.GOV (June 12, 2018), chpl.healthit.gov/#/collections/apiDocumentation (public dataset).

[88] 82 Fed. Reg. 53,568 (Nov. 16, 2017); Seema Verma, Admin'r of Ctrs. for Medicare & Medicaid Servs., Remarks at the HIMSS18 Conference (Mar. 26, 2018), www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2018-Press-releases-items/2018-03-06-2.html.

[89] Aneesh Chopra, Pres., CareJourney, Unleashing Data to Transform Health Care Panel, 2018 EHR National Symposium at Stanford Medicine, at 12:20 (June 4, 2018), youtu.be/qgLlLiabDFU.

party apps to connect,[90] and as a result, may be inappropriately raising their rivals' costs.[91]

An EHR developer's intellectual property is worthy of protection. That protection does not extend, however to the health facts that comprise PHI.[92] Those property rights have limits. For example, a patient's blood sugar test result describes what is occurring in his or her blood. The health fact—blood sugar—may be displayed in a certain manner, with the display potentially being a developer's intellectual property. But the existence of the display does not convert the naturally occurring health fact into the developer's intellectual property.

Furthermore, HIPAA makes it clear that people have a right to obtain form their physicians and hospitals their own PHI, even when extracted from an EHR, and notwithstanding any intellectual property that might exist in the display the developer developed. The patient's right, in existence at least since HIPPA was passed, pre-dates the development of any EHR software IP.[93] Moreover, under HIPAA the developer has no rights to use the PHI for its own business purposes, because under HIPAA, it is merely a business associate.[94]

Data security is another factor that is cited as a barrier to information sharing. HIPAA requires that data must be kept secure. Health care providers are right to want to be confident that health information exchange does not introduce unexpected security risks into their environment, and to look to some extent to their EHR developers to provide a secure environment.[95] But often security and exchange can both be achieved, and providing a secure environment should not be an impediment to exchange.

[90] Arthur Allen, *Developers Complain of High EHR Fees for SMART Apps*, POLITICO (Aug. 6, 2018), www.politico.com/newsletters/morning-ehealth/2018/08/06/onc-interop-forum-kicks-off-306709 (note: a longer version of this publication is available behind Politico's paywall).

[91] Salop & Scheffman, *supra* note 82. R

[92] Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576 (2013). There, the Supreme Court reversed an appellate court ruling that a DNA sequence found in nature could be patented. the Court wrote: "It is undisputed that Myriad did not create or alter any of the genetic information encoded in the BRCA1 and BRCA2 genes. The location and order of the nucleotides existed in nature before Myriad found them. . . . To be sure, it found an important and useful gene, but separating that gene from its surrounding genetic material is not an act of invention." *Id.* at 590–91.

[93] Lucia Savage, *To Combat "Information Blocking," Look to HIPAA*, HEALTH AFF. BLOG (Aug. 24, 2017), www.healthaffairs.org/do/10.1377/hblog20170824.061636/full/.

[94] 45 C.F.R. § 164.504.

[95] OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., DEPT. OF HEALTH & HUMAN SERVS., EHR CONTRACTS UNTANGLED: SELECTING WISELY, NEGOTIATING TERMS, AND UNDERSTANDING THE FINE PRINT 9 (2016), www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf.

In particular, "fake security"[96] concerns should not undermine interoperability or be an excuse for not allowing sharing of information through competing EHR vendors. For example, an open-specification API, such as ONC prescribed in its 2015 edition rule,[97] could be both secure and enable low cost exchange. Indeed, as was clear from evidence presented in public hearings convened by ONC, in most other internet-enabled industries (finance is often the example), businesses and their software engineers and security professionals have adopted methods to keep information flowing while maintaining security.[98] Certainly important regulators, like the CMS Administrator, think EHR developers may have strategically inflated security concerns as a way of impeding exchange.[99]

Last, developers understand there have yet to emerge policies that could counter-balance any urge to hoard data. They may rightly calculate that, without the probability of significant consequences, making exchange hard makes business sense. As we discuss below, there are some steps that can be taken to better understand the impact on health care competition of low levels of information sharing.

C. Factors Affecting Health Care Providers' Information Sharing

No one doubts that physicians, nurses, and the health systems and hospitals in which the majority of health care is delivered want to help their patients. But health care providers and health care systems are businesses, and therefore operate within the realities of the marketplace.[100] We note that while in general federal law does not require providers to exchange data with each other, it does give them quite a bit of flexibility to exchange when they choose to do so. Thus, we explore whether there are incentives on the provider side that explain the low levels of exchange, despite liberal permissions to exchange.

To understand how providers view the competitive implications of information exchange, we turn first to the traditional fee-for-service (FFS) payment system—that is, where the supplier is paid for each service. Doctors and hospitals are sales revenue driven organizations. The overwhelming majority of their revenues come from payments from private insurers and Medicare and

[96] Andy Slavitt, Admin'r of Ctrs. for Medicare & Medicaid Servs., Andy Slavitt and Dr. Karen DeSalvo Panel Discussion at HIMSS (Mar. 14, 2016), www.hitechanswers.net/andy-slavitt-and-dr-karen-desalvo-panel-discussion-at-himss/.

[97] 42 C.F.R. § 170.315(g) (7), (8) & (9).

[98] *See, e.g.*, ONC API Task Force, *supra* note 69, at 27; ESAC Inc. & SRS, Inc., *supra* note 69. R R

[99] Slavitt, *supra* note 96.

[100] Grossman et al., *supra* note 11, at 1. R

Medicaid. As a consequence, providers make money by attracting and retaining (profitable) patients. Making information readily available and transportable helps patients seek out new, and potentially competing, providers. This may make it harder to retain patients and the health insurance fees their care generates. Patients who are mobile may lead to tougher competition among providers. Patients benefit substantially from tougher competition that leads to lower prices and higher quality, but providers are typically worse off.

Furthermore, even as the fee-for-service system evolves to payment for value or population health outcomes, providers who are responsible for a patient's overall care may lose control if a patient receives care outside their system. Thus, even in this type of system, providers may want to keep their patients in the system, even if it is not where the individuals would receive the best or most appropriate care.[101] In principle, it is possible for providers paid on a value basis to contract in a mutually advantageous way for patient care, so that patients are appropriately referred and incentives are maintained. In this situation information sharing is critical—indeed, appropriate and efficient referrals for care cannot take place without it.

As a specific example, Aledade is a start-up seeking to help independent (non-hospital owned) ambulatory practices deliver high-value care using a built-in infrastructure Aledade supplies to enable information exchange. Because Aledade's business model focuses on independent practices collaborating with each other and sharing financial risk for keeping their collective patients out of hospitals,[102] it may prove a counterweight to any tendency of hospital-owned practices to exchange only with other doctors sharing a single information technology system or an integrated ownership structure.[103]

Yet, even information exchange patterns among independent practices can create incentives for a different kind of walled garden, one bounded by referral patterns (instead of proprietary technology), where the institutions choose to allow (or prioritize) disclosure only to specific established electronic ad-

[101] Evidence shows that physician referral patterns are substantially altered when a practice is owned by a hospital, in particular that physician practices owned by a hospital refer substantially more to that hospital than to other hospitals, even if the care at that hospital is of lower quality than elsewhere. Laurence C. Baker, M. Kate Bundorf & Daniel P. Kessler, *The Effect of Hospital/Physician Integration on Hospital Choice*, 50 J. HEALTH ECON. 1 (Dec. 2016) This illustrates that providers respond to incentives (in this example, hospital ownership) by altering their behavior to keep patients in the system.

[102] Brian W. Powers et al., *Engaging Small Independent Practices in Value-Based Payment: Building Aledade's Medicare ACOs*, 6 HEALTHCARE 79 (2018).

[103] Farhad Manjoo, *A Start-Up Suggests a Fix to the Health Care Morass*, N.Y. TIMES (Aug. 16, 2017), www.nytimes.com/2017/08/16/technology/a-start-up-suggests-a-fix-to-the-health-care-morass.html.

dresses, or make it difficult for patients to identify secure electronic delivery locations for data they want sent to their other doctors.[104]

As has been made clear, there are strong financial incentives to retain data and not to share it. In contrast, it is hard to identify a profitable business model that involves information sharing. These concerns about information blocking and provider competition are not merely theoretical. FTC officials blogged in October 2014 about their interest in the implications of provider competition on EHRs and the data they create.[105]

III. CURRENT POLICIES TO ADDRESS DATA BLOCKING

Congress has noticed that health information is not flowing freely among health care providers and has some evidence to suggest that anticompetitive motivations are partly to blame.[106] However, the extent to which anticompetitive conduct is responsible remains unclear, as well as whether such conduct is due to the vendors, the providers, or both. Nor do we know if the incentives hindering exchange of information are symbiotic or merely happen to be contemporaneous. For example, is EHR connectivity costly and difficult because vendors are responding to their provider customers' desires to avoid exchanging data, or would providers be willing to exchange data, but lose interest because of the costs and difficulties with EHR connectivity and compatibility? Are the costs and complexity associated with connectivity legitimate, or are they driven by strategic motives on the part of EHR vendors? What role, if any, do developers' concerns about IP and their security obligations play?

On the provider side, the Meaningful Use regulations continue to require attestation to higher levels of electronic transmission of summary of care records during patient transitions. Specifically, Stage 3 criteria raise the bar from 10 percent to 50 percent, and impose penalties on eligible providers and hospitals that do not meet these thresholds. Nonetheless, thus far Meaningful Use has not been a sufficiently strong driver to result in widespread exchange. Therefore, in January 2015, Congress attempted to further increase incentives when it passed the Medicare Access and CHIP Reauthorization Act of 2015

[104] Keith Boone, *What's My Doctor's Direct Address*, HEALTHCARE STANDARDS (Aug. 18, 2017) (Dec. 16, 2017), motorcycleguy.blogspot.com/2017/08/whats-my-doctors-direct-address.html (an example of making opaque to a patient how to securely transmit PHI to another, unaffiliated provider).

[105] Tara Isa Koslov, Office of Pol'y Planning, Markus Meier, Bureau of Competition & David R. Schmidt, Bureau of Econ., Fed. Trade Comm'n, *Promoting Healthy Competition in Health IT Markets*, COMPETITION MATTERS (Oct. 7, 2014), www.ftc.gov/news-events/blogs/competition-matters/2014/10/promoting-healthy-competition-health-it-markets. *See also* Amalia R. Miller & Catherine Tucker, *Health Information Exchange, System Size and Information Silos*, 33 J. HEALTH ECON. 28 (2014) (finding that large hospital systems strategically prevent outflow of patient data to maintain their competitive advantage).

[106] *Senate Information Blocking Hearings*, *supra* note 81. R

(MACRA).[107] This Act replaced the old Medicare payment formula with a sweeping new payment method that requires payments for Medicare physician services be based on value and measured outcomes. These measures and outcomes, in turn, were to be specified in regulations.[108] The resulting regulations for payment years 2017 and 2018 increase the amount of care that is paid based on measured outcomes, and those outcomes are calculated in part using the digital health data HITECH made widely available.[109] Among the new measures is an attempt to measure exchange as part of the "advancing care information" domain.[110] To achieve top marks in this domain for calendar 2017, however, a physician needed only exchange a summary of care record with a single other physician.[111] For calendar 2019, CMS proposes only that hospitals need prove information exchange on behalf of only one individual.[112]

Despite enacting MACRA in late 2015 (with more incentives payable for exchange but no explicit provisions on information blocking), it appears that Congress remained concerned that information was still being blocked. After holding three hearings on the subject of information blocking,[113] in December 2016, it enacted Cures, which contains elements designed to address this issue directly.[114] Cures itself defines "information blocking," and charged HHS with identifying conduct that is not "information blocking" and rooting out and punishing information blocking when it occurs.[115]

Specifically, 21st Century Cures says that a practice is information blocking: ''(ii) if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or mate-

[107] Pub. L. No. 114–10, 129 Stat. 87 (2015) (codified in scattered sections of 42 U.S.C.) [hereinafter MACRA].

[108] MACRA regulations for physician payment are published as part of the Medicare Physician Fee Schedule rules, and are updated annually. *See* 42 C.F.R. § 495. There are corollary rules for hospitals published in the Medicare Inpatient Prospective Payment System rule, also updated annually. *See* 42 C.F.R. § 412 as finalized in the rule published at 83 Fed. Reg. 41,144 (Aug. 17, 2018).

[109] 82 Fed. Reg. 53,568, 53,570 (Nov. 16, 2017). Measures and relation to certified EHR technology are explained at CMS, *2018 Promoting Interoperability*, QUALITY PAYMENT PROGRAM, qpp.cms.gov/mips/explore-measures/promoting-interoperability?py=2018#measures.

[110] CMS Quality Payment Program, *Merit-based Incentive Payment System (MIPS): Participating in the Advancing Care Information Performance Category in the 2017 Transition Year*, www.cms.gov/Medicare/Quality-Payment-Program/Resource-Library/MIPS-Advancing-Care-Information-101-Guide.pdf.

[111] CMS, *Promoting Interoperability (PI) Requirements*, QUALITY PAYMENT PROGRAM, qpp.cms.gov/mips/advancing-care-information (CMS explanation measures under its Quality Payment Program).

[112] 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 20,164, 20,550 (proposed May 7, 2018), 83 Fed. Reg. 41,144, 41,637 (Aug. 17, 2018).

[113] *See Senate Information Blocking Hearings*, *supra* note 81. R

[114] Cures, *supra* note 5, §§ 4001–4006, 130 Stat. 1157–1183 (codified in scattered sections of 42 U.S.C.). R

[115] *Id.*

rially discourage access, exchange, or use of electronic health information." And it defines information blocking by developers as behavior that "if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information[.]"[116] Providers will be permitted to attest that they have not blocked information; EHR vendors, however, will have to demonstrate that they have not information blocked in response to standards developed by the Secretary.[117] Cures also authorizes fines against EHR developers of up to $1 million.[118]

In addition, the HHS Office of the Inspector General (OIG) is using existing regulations to target data blocking by vendors. On May 31, 2017, the OIG and the DOJ's fraud unit settled for $155 million a case against eClinicalWorks, an EHR developer, under the False Claims Act. The government alleged in part that the developer's "software failed to satisfy data portability requirements intended to permit health care providers to transfer patient data from eClinicalWorks' software to the software of other vendors."[119] eClinicalWorks is one of the top 10 EHR developers in the United States by size.[120] The next day, OIG issued a report estimating that over $700 million in Meaningful Use incentives had been paid based on meaningful use stage 1 and 2 attestations that OIG could not verify based on a random sample. Those attestations, including attestations that exchange occurred with unaffiliated organizations.[121]

States have concurrent jurisdiction over, and their own interest in, a competitive health care landscape. States are empowered to take action, and one has. Following the publication of ONC's Information Blocking Report, Connecticut enacted a law that includes specific requirements for easily moving

[116] *Id.* § 4004(a)(1)(B) (codified at 42 U.S.C. 300jj–52(a)(1)(B)).

[117] *Id.* § 4004(a)(3) (codified at 42 U.S.C. 300jj–52(a)(3)).

[118] *Id.* § 4004(b)(2)(A) (codified at 42 U.S.C. 300jj–52(b)(2)).

[119] Press Release, U.S. Dep't of Justice, DOJ Settles False Claims Act with eClinical Works, (May 31, 2017), www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.

[120] *eClinicalWorks Holds Highest Market Share for Ambulatory Cloud-Based EHRs,* BECKER'S HOSP. REV. (Jan. 26, 2016), www.beckershospitalreview.com/healthcare-information-technology/eclinicalworks-holds-highest-market-share-for-ambulatory-cloud-based-ehrs.html.

[121] DANIEL R. LEVINSON, INSPECTOR GEN., DEP'T OF HEALTH & HUMAN SERVICES, MEDICARE PAID HUNDREDS OF MILLIONS IN ELECTRONIC HEALTH RECORD INCENTIVE PAYMENTS THAT DID NOT COMPLY WITH FEDERAL REQUIREMENTS (June 2017), oig.hhs.gov/oas/reports/region5/51400047.pdf. One finding was that 12% of stage 1 Meaningful Users inaccurately attested. Stage 1 included the requirement of at least one instance of exchange. *Id.* at 16.

health information from one provider to another.[122] According to state Senator Martin Looney, one of the bill's sponsors:

> [H]ospital systems in Connecticut have been pressuring independent physician practices to join their network by denying them electronic access to a patient's full medical records unless they join. [Looney] said these health systems, namely Yale New Haven Health and Hartford Health, have used their Epic Systems-made EHRs to create a private health information exchange accessible only to affiliated providers or those providers willing to pay thousands of dollars to connect to the hospitals' IT systems. "Epic has become a monopolistic practice," Looney said. "If you're not part of Epic through the hospitals you're left out and your practice is at a great disadvantage."[123]

In other words, State Senator Looney was concerned that the "walled gardens" described in ONC's report were simply becoming bigger on the inside, and that dominant hospital systems were intent on creating technology captives among their physicians with admitting privileges and those physicians' patients. Whether the Connecticut law will be successful at breaking down the walls remains to be seen.

IV. NEW POLICIES TO PROMOTE DATA SHARING

There is a strong public policy rationale for more freely flowing information. Freely flowing information between providers will make patients more mobile and promote competition between providers. Further, improved provider data sharing will improve care coordination, which should enhance quality of care and could reduce costs. Greater EHR interoperability will also promote the flow of information and the benefits that accrue from it. Finally, enhanced interoperability should increase competition between EHR vendors.

As indicated above, policymakers have taken some important initial steps, but there are some additional things that can be done to help improve matters.

First, we suggest that the FTC conduct a study of the exchange of health data and whether health information exchange is being impeded because of attempts to avoid competition. We know that less health data are being exchanged than expected or desired, but we need to know more about what is happening, what actions specifically are being taken by organizations that affect data sharing, and how these affect competition. Specific information could be collected such as (but not limited to the following):

[122] An Act Concerning Hospitals, Insurers & Health Care Consumers, 2015 Conn. Pub. Act 15-146.

[123] Alex Ruoff, *In Connecticut, Debate Starts over Information Blocking*, HEALTH IT LAW & INDUSTRY REPORT (BLOOMBERG/BNA) (Nov. 9, 2015) (on file with authors).

(1) How many health information exchange transactions occur between unaffiliated EHRs or among providers who are not in the same medical group or corporate family in a wide variety of markets?

(2) When information sharing occurs, what are the costs and the benefits the EHR vendors or providers experience? What is it that makes it beneficial for the various parties to the exchange? What are the key factors that support exchange?

(3) When information sharing does not occur, what are the costs and benefits? What is it that does not make it beneficial for parties to the potential exchange? What are the key factors that prevent exchange?

(4) How frequently is HIPAA used as a justification for not exchanging when, under the HIPAA regulations, exchange would be permitted and no other privacy laws apply?

(5) What are the costs incurred in engineering connectivity between two different EHR systems for two providers who want to exchange data?

(6) How frequently are developers of third-party apps authorized to connect to the open-specification API that ONC included in its 2015 regulation and, if the developer has to pay for that privilege, what are the prices the developer pays?

(7) What are the fees data holders charge for transmitting data? How do those fees correspond to the costs of transmitting data? Does it appear that data holders are setting fees at high levels in order to deter demand for data or to raise the costs of rivals to put them at a competitive disadvantage?

(8) What action are private payers taking to ensure their enrollees have their data available for all clinicians, particularly across institutions or EHR systems?

Further, in the period since the passage of HITECH, some health care mergers have been defended in part by citing the need for integrated, uniform health IT systems to improve efficiency and quality.[124] We need to know more

[124] *See* Respondent's Answer at 12, Advocate Health Care Network, FTC Docket No. 9369 (Jan. 5, 2016), www.ftc.gov/system/files/documents/cases/advocate_healthcare_respondent_northshore_university_health_systems_answer_to_administrative_complaint_580478.pdf (responding to FTC Admin. Complaint ¶ 48 (Dec. 17, 2015), www.ftc.gov/system/files/documents/cases/151218ahc-pt3cmpt.pdf (provisionally redacted public version)); *see also* Complaint at 3, 13 & 14–16, Penn State Hershey Med. Sys., FTC Docket No. 9368 (Dec. 7, 2015), www.ftc.gov/system/files/documents/cases/151214hersheypinnaclecmpt.pdf (provisionally redacted public version); Fed. Trade Comm'n Staff, Submission to the Southwest Virginia Health Authority and Virginia Department of Health Regarding Cooperative Agreement Application of Mountain States Health Alliance and Wellmont Health System 33–36 (Sept. 30, 2016), www.ftc.gov/sys

about the existence and magnitude of such efficiencies, the extent to which they are merger specific, as well as any impacts they have on competition.

If the information to answer these questions is readily publicly available, then the FTC can conduct a study using those sources. If the information is not readily publicly available, the FTC can use its powers in Section 6(b) of the Federal Trade Commission Act[125] to obtain the relevant information from those possessing it.[126]

Second, while the FTC's role is significant, it is important to remember that only the DOJ has federal enforcement jurisdiction over anticompetitive practices by non-profit corporations,[127] including the 58 percent of hospitals that are non-profits.[128] These non-profit hospitals are custodians of significant quantities of clinical digital health information. Therefore, through its long collaboration with FTC,[129] the DOJ can use the results from any FTC study or FTC enforcement actions to evaluate whether there is information blocking that rises to the level of an actionable enforcement issue for non-profit health care actors.

Third, ONC and CMS can take actions to promote the adoption of the information technology that is used throughout the rest of the economy for internet-enabled transactions. For example, while ONC cannot require the

tem/files/documents/advocacy_documents/submission-ftc-staff-southwest-virginia-health-authority-virginia-department-health-regarding/160930wellmontswvastaffcomment.pdf (rebutting claims that adopting unified EHR system is necessary to share patient data to achieve quality improvements); Fed. Trade Comm'n Staff, Supplemental Submission to the Tennessee Department of Health Regarding the Certificate of Public Advantage Application of Mountain States Health Alliance and Wellmont Health System 17–18 (Jan. 5, 2017), www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-supplemental-submission-tennessee-department-health-regarding-certificate-public-advantage/170105mshatennesseesuppcmt.pdf.

[125] 15 U.S.C. § 46.

[126] Section 6(b) of the FTC Act "empowers the Commission to require the filing of 'annual or special reports or answers in writing to specific questions' for the purpose of obtaining information about 'the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals' of the entities to whom the inquiry is addressed." Fed. Trade Comm'n, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority* (July 2008), www.ftc.gov/about-ftc/what-we-do/enforcement-authority (quoting 15 U.S.C. § 46).

[127] The FTC's jurisdiction over non-profits is limited by the definition of corporation in Section 4 of the FTC Act, which includes those entities "organized to carry on business for [their] own profit or that of [their] members." 15 U.S.C. § 44. Thus, while FTC has authority under the Clayton Act to challenge mergers of non-profit corporations, it cannot assert jurisdiction over non-profits in other types of antitrust cases.

[128] Brooke Murphy, *Fifty Things to Know About the Hospital Industry 2017*, BECKER'S HOSP. REV. (Jan. 25, 2017), www.beckershospitalreview.com/hospital-management-administration/50-things-to-know-about-the-hospital-industry-2017.html.

[129] Bill Baer, Assistant Att'y Gen., Antitrust Div., U.S. Dept. of Justice, Remarks at The New Health Care Industry Conference, The Role of Antitrust Enforcement in Health Care Markets (Nov. 13, 2015), www.justice.gov/opa/file/794051/download.

adoption of any particular technology, it can continue to champion technologies that facilitate low-cost interoperability, such as open-specification (non-proprietary) Application Programming Interfaces (APIs).[130] If used, this could drastically reduce the technical friction of secure, auditable information sharing. CMS's role is to financially incentivize use of the technology ONC requires of certified EHR systems. Starting in January 2019, CMS will require physician practices (as a condition of payment for services delivered to Medicare beneficiaries) to use the open API.[131] Specifically, the open API will enable, from a technical perspective, authentic and secure apps from unaffiliated businesses to access EHR data for legitimate purposes, as already occurs in finance and retail.[132] Since adoption of the open API will drastically reduce technical barriers to exchange,[133] if information flow is not substantially increased thereafter, persistent low levels of exchange will make a strong case that information hoarding is occurring, impeding competition. Such evidence may warrant investigation by federal or state antitrust authorities.

Fourth, ONC and CMS could more aggressively create financial incentives for providers to engage in exchange by tying provider payments to process and outcome measures that are directly affected by the level of information exchange. ONC has taken an initial step in this direction by funding the National Quality Forum to begin to develop such measures, and the resulting set of measure concepts span both exchange activity (e.g., percentage of available structured elements that were electronically exchanged per patient) and outcomes that are likely to be improved by exchange (e.g., percentage reduction in duplicate labs and imaging over time).[134] These were only concepts, how-

[130] Consistent with its mission to facilitate nationwide health information exchange, ONC in 2015 updated its software rule to require that to be certified by ONC, a developer had to include an open-specification, i.e., read-only "Application Programming Interface," which would enable unaffiliated application developers to write apps to extract (read-only) data from one system and transport it elsewhere. 42 C.F.R. § 170.315(g)(7) (2015). Unfortunately, in its most recent proposed rules on expected behavior by hospital and providers to earn incentive payments or to avoid penalties, CMS did not require that hospitals or providers allow this API to be used, whether by individuals to get their own health data (as is required by law, 82 Fed. Reg. 30,010, 30015 (June 30, 2017)), or by allowing an app to work to exchange with an unaffiliated physician for a shared patient, both of which HIPAA has always allowed. *See HIPAA Fact Sheets*, *supra* note 25. **R**

[131] 45 C.F.R. § 170.315(g)(9) (2015) states the API certification rule. CMS delayed required use by Eligible Physicians and by the Eligible Hospitals until 2019, but has finalized this deadline. 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 41,144, 41,637 (Aug. 17, 2018). *See also* 2018 Medicare Physician Fee Schedule Rule, 82 Fed. Reg. 52,356 (Nov. 13, 2017); Medicare 2018 Inpatient Prospective Payment Rule, 82 Fed. Reg. 37,990 (Aug. 14, 2017).

[132] ONC API TASK FORCE, *supra* note 69. **R**

[133] *Id.*; *see also* 2015 Edition ONC Certified Electronic Health Information Technology, 80 Fed. Reg. 62,601, 62,675–79 (Oct. 16, 2015).

[134] NAT'L QUALITY FORUM, A MEASUREMENT FRAMEWORK TO ASSESS NATIONWIDE PROGRESS RELATED TO INTEROPERABLE HEALTH INFORMATION EXCHANGE TO SUPPORT THE NATIONAL QUALITY STRATEGY (Sept. 1 2017), www.qualityforum.org/Publications/2017/09/Interoperability

ever, and no such measure specifications presently exist. Moreover, it is not clear who will take up the work to develop the measures and shepherd them through the endorsement process so that they can be used in practice. Typically, development of measure specifications is undertaken in response to a robust evidence base by government agencies or private nonprofits, and resulting measures are then endorsed by professional societies and/or consumer groups.[135] While the evidence base for the benefits of exchange is expanding, it is still fairly limited and, because information exchange cuts across so many contexts and clinical conditions, it does not have an obvious set of stakeholders to take on the development or pursue subsequent endorsement. Of course, the benefits and costs of such enhanced financial incentives should be evaluated carefully before adopting such a policy.

Making funding available to entice measure developers to speed the creation of promising measures may also be worthwhile. In the interim, a practical option, but one with potential unintended consequences, could involve tying stronger financial incentives to existing measures of performance that are likely to reflect high levels of information exchange. For example, there is a measure in the Hospital Consumer Assessment of Healthcare Providers and Systems "Clinician & Group" survey that asks patients about whether their provider had access to all prior information about their care.[136] Tying CMS provider payment to high performance on this measure, or a close derivative of it that asks about prior information from "external" providers, could be a powerful driver of greater information exchange (as well as ensuring that information is not only exchanged, but is also made easily available to frontline providers at the point of clinical decision making).

While such incentives would serve as a powerful counterbalance to current incentives not to share data, it is important to recognize that this approach could also be gamed or have unintended negative consequences. For example, if only some providers are subject to these payment incentives, it could create a scenario in which the providers that need to engage in exchange to meet the measure are beholden to another set of providers who do not need to meet the measure but care for the same patient population. In this scenario, the latter group, which hold the patient data needed for high measurement achievement would have leverage over the former group. That leverage might even inten-

_2016-2017_Final_Report.aspx (pursuant to contract HHSM-500- 2012-00009I, Task Order HHSM-500-T0021).

[135] FamiliesUSA, *Measuring Healthcare Quality: An Overview of Quality Measures* (May 2014), familiesusa.org/sites/default/files/product_documents/HSI%20Quality%20Measurement_Brief_final_web.pdf.

[136] Agency for Healthcare Research & Quality, *CAHPS Clinician & Group Survey* (July 1, 2015), www.ahrq.gov/sites/default/files/wysiwyg/cahps/surveys-guidance/cg/survey3.0/adult-eng-cg30-2351a.pdf.

sify any existing market consolidation pressures (i.e., formally aligning with or acquiring a provider group in order to achieve the measure through exchange).

Fifth, there is a role for payers in promoting information exchange. For example, Intel Corporation in 2013–2015 experimented with creating a narrow network for its employees (in certain locations where it was a dominant employer), where participation in the network required providers to exchange data with each other.[137] While Intel apparently had good results on quality improvement and cost savings, its approach has not been widely duplicated. It is not clear why private payers generally have not been more aggressive in pursuing such strategies.

There are some counterexamples. Interestingly, Blue Shield of California recently announced that in order to contract with it in-network, providers had to also exchange data through the California state HIE, at no cost to the providers.[138] Furthermore, for accountable care organizations (ACOs) and other value-based payment models to take root in the private sector, health information must be exchanged. Organizations like the public-private "learning and action network" and commercial payers are working towards wider adoption of alternative payment models, and recognize that data sharing is "foundational for operationalizing" such models.[139] To date, however, their work is still in an early stage. Finally, although some state Medicaid agencies and commercial payers have used their oversight and market powers to accelerate the rate of health information exchange,[140] this approach is not widespread.[141] In spite of these examples, for the most part payers have not taken an active role in promoting information exchange. The role of payers is not well under-

[137] Prashant Shah, Angela Mitchell & Brian DeVore, Intel Corp., *Advancing Interoperability in Health Care: Employer Led, Standards-Based Collaboration to Advance the Triple Aim* (2015), www-ssl.intel.com/content/www/us/en/healthcare-it/solutions/documents/advancing-interoperability-healthcare-paper.html.

[138] Press Release, Blue Shield of Cal., Blue Shield of California Commits to Work with Providers to Bring Health Care into the Digital Age (Mar. 6, 2018), www.businesswire.com/news/home/20180306006518/en/Blue-Shield-California-Commits-Work-Providers-Bring.

[139] HEALTH CARE PAYER LEARNING & ACTION NETWORK, ACCELERATING AND ALIGNING POPULATION-BASED PAYMENT MODELS: DATA SHARING (Aug. 8, 2016), hcp-lan.org/groups/pbp/ds-final-whitepaper/.

[140] *See* Governor of Ohio, Office of Health Transformation, *Ohio Medicaid Reform* (Aug. 2015), healthtransformation.ohio.gov/Portals/0/OhioMedicaidReforms8-11-2015.pdf?ver=2015-08-17-142316-027; Blue Cross Blue Shield of Mich., *2017 PGIP Fact Sheet: Health Information Exchange Initiative*, VALUEPARTNERSHIPS.COM (Mar. 2017), www.valuepartnerships.com/wp-content/uploads/2017/03/2017-HIE-Initiative-Fact-Sheet.pdf. Medicaid is a complex system in its own right, given federal funding and state eligibility rules, and a deeper discussion of Medicaid and information exchange or information blocking is beyond the scope of this article.

[141] Dori A. Cross, Sunny C. Lin & Julia Adler-Milstein, *Assessing Payer Perspectives on Health Information Exchange*, 23 J. AM. MED. INFORMATICS ASS'N 297 (2016).

stood, and as indicated above, could be a valuable subject for investigation by an FTC study.

V. CONCLUSION

While there is widespread agreement on the benefits from routine sharing of digital health data, and specific federal goals that seek to achieve it, data sharing is still the exception rather than the rule. As we have indicated, EHR vendors and providers likely find it to their advantage to refuse to share data with rivals. While this is understandable, it can harm competition and consumers.

Furthermore, while these issues are important now, we expect them to only grow in importance. Our world is being transformed to one in which data are central to individuals and businesses. This digital transformation is coming to health care the same way it has come to much of the rest of the economy. In this state of the world, the portability of data, or lack thereof, may become a major driver of competition, costs, and outcomes. We need to better understand the factors driving the current lack of health data exchange and formulate policies that facilitate its use and transmission to benefit society.

ONC's Proposed Rule On Information Blocking: The Potential To Accelerate Innovation In Health Care, HEALTH AFFAIRS BLOG, February 15, 2019. DOI: 10.1377/hblog20190215.3077
Copyright 1995 - 2019 by Project HOPE: The People-to-People Health Foundation, Inc., eISSN 1544-5208.

Lucia C. Savage, JD

FEBRUARY 15, 2019
10.1377/HBLOG20190215.3077

In 2015, when the Office of the National Coordinator for Health IT (ONC) – where I served as chief privacy officer at the time -- started planning what would become the “open specification API” rule of ONC’s 2015 Edition Certification Rule, we purposefully grounded that rule, and the corollary CMS rule (now called “promoting interoperability”), on an individual’s right to get, use and send their protected health information. We did so because this right cannot lawfully be denied. Unlike information sharing between health care businesses (B2B), which is permitted but not required, disclosure to an individual is *required*. Driven by the vision that this strategy would help APIs take root and flourish in healthcare, we hoped that over time, apps and APIs would be used for exchange of information B2B, and not just in disclosures to consumers (B2C).

Now, with the recent publication of the Notice of Proposed Rulemaking to Improve the Interoperability of Health Information (NPRM), ONC and Health and Human Services (HHS) have firmly committed themselves to this vision. ONC made specific proposals for how apps and APIs could be used B2B for extraction and transport of data on whole patient populations, not just for an individual’s needs. Bravo, ONC, for this bold proposal. As a proposed rule, however, it remains to be seen how many of these big ideas remain in ONC’s final rule. The public comment period on this rule closes 60 days after the rule officially publishes in the Federal Register, with a comment deadline of approximately April 11. For more detail on the NPRM, visit the fact sheets on ONC’s website.

The NPRM has the potential to advance interoperability in surprising ways, while preserving privacy. The NPRM covers many additional topics including: pediatric EHRs; technical rules for maintenance of certification, attestation and testing and a prohibition on “gag” clauses; a request for information on clinical registries; revisions to the “common clinical data set” that include new categories of data and a new method for updating this minimum data set; and which version of the Fast Health Information Resource should be required to be used. Such topics are beyond the scope of this post. Below, I will outline a few aspects of the rule, and note a few policy-oriented provisions that bear watching.

Provisions To Watch

For context, this NPRM was released one day before final comments were due on the HHS Office for Civil Rights (OCR) Request for Information on Modifying HIPAA Rules To Improve Coordinated Care. OCR sought input on 54 questions about potential changes to the HIPAA Privacy Rule which might advance care coordination and dovetail to ONC’s proposals. The ONC

NPRM was released simultaneously with a CMS proposed rule that, if enacted, would make it a condition of participation that "that Medicaid, the Children's Health Insurance Program, Medicare Advantage plans and Qualified Health Plans in the Federally-facilitated Exchanges *must provide enrollees with immediate electronic access to medical claims* and other health information electronically by 2020."

Improving care coordination has been a top priority for HHS, as demonstrated by their commitment to empowering patients through the MyHealthEData campaign, and ensuring that taxpayers get more value from the $37 billion in incentives to use electronic health records. Accordingly, the NPRM focuses on implementing the presumption in The 21st-Century Cures Act (Cures) that there are *very few* circumstances when exchange of electronic health information (EHI) should not occur. It lists seven activities which, when they occur, would not be considered "information blocking" prohibited by Cures: (1) preventing harm; (2) promoting privacy; (3) promoting security; (4) Recovering costs reasonably incurred to make the API technology available; (5) infeasible requests for data; (6) License conditions that the data discloser or API technology supplier imposes on the app developer and which are reasonable and non-discriminatory; and (7) system maintenance.

Among the seven activities listed, preventing harm, promoting privacy, and promoting security are to be expected on this list. One specific element of the promoting privacy exclusions, however is worth noting and watching in the final rule. ONC proposes that it would not be information blocking for an organization to follow, according to the fact sheet, "certain practices not regulated by HIPAA but which implement documented and transparent privacy policies [of the organization]". However, as ONC itself pointed out in its 2015 Interoperability Roadmap (page 18), sometimes it is organizational policies and unduly restrictive or even incorrect interpretations of HIPAA or state privacy law that lead to a lack of interoperable movement of information. Here, despite its 2015 diagnosis, ONC seems to be allowing organizations to continue to comply with internal policies, however well or ill founded. The worry here is that in cases where an organizational policy misapplies legitimate privacy laws as a pretext for business decisions to not share, such conduct would still not be considered information blocking. See, e.g. Savage, L, Adler-Milstein, J., and Gaynor, M, "*Digital Health Data and Information Sharing: a New Frontier for Health*" forthcoming in 82 American Bar Association Antitrust Law Journal p 701, at 706) (March 2019).

Another area that bears watching is ONC's proposals for recovery of reasonably incurred fees and for license conditions that could be imposed on the apps using the required APIs. The proposed rules in this portion are complex. The way ONC officials described it at HIMSS 2019 this week, some fees could be negotiated by the API technology supplier (aka EHR developer) and the API data discloser (aka the health care provider or plan) but charged to the app developer who is accessing the data held by the data discloser. However, the app developer, will not have been a party to the price negotiations. One can well imagine different ideas of "affordable" and "reasonable" as between a start-up and a multi-site health system or a multi-billion-dollar EHR developer. Yet, to obtain the competitive, innovative health care ecosystem ONC and HHS explicitly desire, prices cannot be so high as to themselves be a barrier (this concept is discussed at length in Savage, et al., cited above). And, while the Federal Trade Commission has significant authority to address price-setting that may be anti-competitive, the process of doing so takes many years.

Furthermore, as I have written previously, HIPAA does not permit organizations to monetize protected health information. ONC has attempted to address this by articulating when an API technology supplier or data provider may NOT recover fees. But, it remains to be seen whether incumbent health care stakeholders, who have financial incentives to not let their patients get care elsewhere, can develop cost recovery schema that do not monetize PHI impermissibly, and that enhance competition. While ONC has proposed careful detail about what licensing means, (highlighted in this detailed fact sheet), EHR developer efforts to protect intellectual property via licensing have heretofore interfered with interoperability, as ONC itself acknowledges.

Patients' Perspective

For patients, the NPRM offers two significant improvements. First, while it is clear that reasonable fees that are not anti-competitive *may* be charged to app developers, especially for apps using the NPRMs B2B features, individuals are not to be charged when they use an app to get their own PHI. Second, ONC has added to its certification criteria that certified EHRs must make use of an HL7-approved standard for marking certain data as subject to special handling for privacy reasons. This standard is known as Data Segmentation for Privacy, or "DS4P". With this technology in place, health care providers will be able to more automatically ensure that special data -- such as that from an Opioid Use Disorder program or the reproductive health data of a teenager -- is handled in a manner consistent with the special privacy rules that apply to it. Another instance of special data is the privacy choices offered by an organization to individuals – that is, granular privacy choices such as "share with my sister but not my ex - husband". DS4P could also be used to document such a choice. An individual's privacy choice, when given a choice, is different from an organizational policy. Individual choices reflect the specific privacy choices are one person makes to help them manage their health, and are highly unlikely to be anti-competitive. Organizational policies reflect the organization's desires and business operations. As discussed above, business policies may be based on privacy, but may veer into anticompetitive intent, which should not be allowed.

Bringing an app enabled eco-system to life in health care would change many things. It would advance innovation in: where care is delivered, how care is delivered, how we understand the healthcare needs of individuals, and how we make sure health care professionals have all the information they need when collaborating for care with patients. The HITECH act is just ten years old, and investments in health IT did indeed unleash economic stimulation of new care delivery modes. ONCs information blocking rule has real potential to accelerate that innovation.

omada

February 10, 2019

Roger Severino, JD
Director,
HHS Office for Civil Rights
200 Independence Ave, SW
Washington DC 20201
By Electronic Submission

RIN: 0945-AA00

Dear Director Severino:

Omada Health, Inc., respectfully submits the below comments in response to the U. S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Request for Information (RFI) dated December 14, 2018 (HHS-OCR-0945-AA00).

Omada Health, Inc. (Omada) is one of the nation's largest digital health care service providers. Founded in 2011, Omada provides health care services (as defined in 45 CFR 160.103) by connecting professional coaches to individuals through a secure communications platform. That platform allows our professional coaches to use clinically validated intensive behavioral counseling techniques and related services for clinically validated activities such as:

- Diabetes Prevention Program (DPP)[1],
- Diabetes self-management education,
- Coaching for hypertension management, and
- Coaching for medication adherence.

Within the next 12 months, we will also expand our services to deliver care for individuals dealing with anxiety and depression. We are the largest DPP in the country to have achieved CDC full recognition, and have served over 200,000 people from age 18 beyond age 65 in our eight-year history.

[1] The criteria for what constitutes a CDC Fully Recognized DPP and which programs are fully recognized can be found at: https://nccd.cdc.gov/DDT_DPRP/Registry.aspx

As a health care services provider as defined by 45 CFR 160.103, we have since our founding operated as, and considered ourselves to be, a covered entity under the Health Insurance Portability and Accountability Act (HIPAA). In 2016, the Centers for Medicare and Medicaid Services (CMS) reiterated what we had always known: that entities that provide health care services using secure 21st Century digital communications services are still providing health care services within the meaning of HIPAA. 81 Fed. Reg. 80170, 80472 (Nov 16, 2016).

As a provider and covered entity, albeit one that provides services using the latest digital health, sensors, and data science for population health analytics and to personalize how our we deliver our health care services, we are pleased to provide what we hope is helpful information set forth below.

I. INTRODUCTION

At Omada, we have built an outcomes-based reimbursement model utilizing HIPAA rules as a foundation. The statute enables sharing of PHI for program evaluation, care coordination and quality improvement. For customers that contract on outcomes-based pricing, we provide the minimum necessary data to validate clinical success and enable our claims-based billing. We also believe that the way HIPAA permits but does not require sharing of PHI with other covered entities appropriately balances the dignity of individuals with standard rules that keep the health system running.

When OCR finalized the Privacy Rule in 2002, claims data was quite structured, but clinical data was not. Since then, Congress enacted the Health Information Technology for Clinical Health Act (HITECH) and the Meaningful Use (now Medicare Incentive Payment System, or MIPS) program, which vastly changed the quantity of structured clinical data. Also, since 2009, advances in computing and smart phone/mobile technology have resulted in new sources of digital clinical data, while significantly lowering barriers to collecting that data.

While many features of the Privacy Rule are resilient and flexible because they specify required outcomes, other features could be updated to help individuals, covered entities, and health care innovators better understand and comply with the important dignitary rights embodied in the Privacy Rule.

First, OCR should consider updating in a rule, or publishing sub-regulatory guidance, that accounts for the fact that PHI now consists of health facts about an individual (like blood sugar test result ratio), as well as metadata and other data structural components that have nothing to do with health facts. Separating these concepts out in regulation will, as we describe in section II.A., help OCR and HHS improve disclosure back to individuals and improve subsequent sub-regulatory guidance as well as HHS ability to promulgate future revisions to existing rules.

Second, any changes that OCR proposes or enacts should advance towards convergence with other privacy standards, including those from FTC, HHS OIG, or FDA SaMD.[2] By bringing standards from various agencies in line, the federal government will create a more easily understood set of standards. This will benefit consumers and accelerate innovation[3].

Within the framing that the two bookended recommendations above provide, we offer the following substantive comments.

II. SUBSTANTIVE COMMENTS

A. HIPAA's Definition of PHI Should Match and Keep Pace With Regulatory Standards for How Health Information Is Structured.

Congress enacted HIPAA in 1996 to usher in an era of electronic billing by physicians and hospitals of federal programs. In 1996, and even in 2000 and 2002 when HIPAA Privacy regulations were first finalized, digital health information was in its infancy. The only digital information available were sets of data that contained demographic information, CPT and ICD Codes. These codes provided an important cumulative picture of the care for which a provider sought payment. With the advent of digital claims data and the HIPAA Transactional Code Sets, health care stakeholders were, for the first time, able to effectively find patterns in the data that related to the process of care. With the advent of the Health Care Effectiveness Data Information Set (HEDIS) came rudimentary measures of the actual care that was billed. We still lacked the ability to measure how effective the care was, relative value of different types of care on outcomes, or to easily share and use clinical records across a team of healthcare professionals who might even be in physically disconnected locations.

The 2000 and 2002 Privacy and Security regulations clearly prescribed how physicians, hospitals, nurses and other professionals could share data across institutions in ways that the vast majority of individuals expected would occur,[4] including treatment and care coordination. See the specific rules at. 45 CFR 164.506(c)(1). These rules are data format neutral. They apply to PHI whether on paper, in a fax, or electronic. As to electronic health information, they apply to all types, from CPT codes to the type of health information that Omada collects. These rules also presciently anticipated a value-based healthcare system, providing leeway for providers to share information to payers (and vice versa) for a recipient's ability to understand, measure, evaluate and improve the quality of health care delivery. 45 CFR 164.506(c)(4). Through these rules, the U.S. system of choice and private insurance ran; individuals did not have to stop their

[2] The Food & Drug Administration "Software Precertification Program: A Working Model" v. 1.0 published January, 2019, includes evaluation of both an organization's cybersecurity processes and culture and its data integrity [acdd cites]. This is appropriate given the technical convergence of the Internet of Things in Healthcare. See also [FTC report on Healthcare IOT]

[3] Cite Non -Covered Entity Report.

[4] See Letter of Privacy Tiger Team of the federal Health Information Technology Policy Committee to the National Coordinator for Health IT dated September 1, 2010, page 4, found at: https://www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10.pdf.

busy lives to give permission to a physician to send a bill to the individual's insurance company. In 2000 and 2002, however, clinical data was almost entirely unstructured.[5]

At present, clinical data is highly structured, and not just in certified electronic health records regulated by HHS. Today, structured, clinically informative health data exists widely throughout the healthcare system, and generally consists of health facts about each individual (for example a name, a complete date, a clinical marker such as an CPT code or a code for a prescription). Todays' clinical data also consists of many other data elements that make the clinical markers useful, but are not themselves clinically indicative. From our perspective, neutral to any particular platform or digital health product, we see several functions occurring in digital data, as follows:

1. **Core Health Facts:** digital information that illustrates or describes core health conditions for an individual from lab test results to diagnoses to physician notes or patient generated health data.
2. **Peripheral/Non-Core Health Facts**: health care providers, and especially digital providers collect a lot of data that, while it is about the individual, and is collected by a health care provider, is not core to the patient's health. For example, Omada collects individuals exercise information when the individual authorizes it. This helps engagement and individual accountability, but a step count alone does not tell our CDE coaches how well managed a diabetic's blood glucose is.
3. **Operational Facts**: digital providers generate a variety of operational facts that are useful for the operations and efficiency of the provider, but provide little value for the patient. As an example, if a patient loses access to a provider's portal and needs to perform a password reset, this may create operational facts. These facts are tied to the patient but offer no value to the patient from a health care perspective. Knowing if operational facts were "protected health information" and part of a 'designated record set" would help entities that generate these operational facts know what was legally required.
4. **Metadata**: digital providers and traditional providers who use certified electronic health records systems generate a large volume of metadata (data about data) during the natural course of providing care. As an example, an audit log may contain metadata including a patient's IP address, unique identifiers, specific features the patient accessed (how the individual used the digital tool), time and date stamps, and error codes. This data is often unstructured and used to operate the digital platform, but not for patient care. These data are quite useful for maintaining data integrity and for leaving a trail that can be followed should the Core Health Facts be inappropriately accessed or disclosed. But these data are not directly related to an individual's health the way a weight, diagnostic code, or lab value is.
5. **Metadata tags**, which may help an organization sort, compile and analyze data and is connected to health facts, but is not itself a health fact or even about an individual. Tagging like this can help a data holder know what is permitted or not, such as the "data

[5] See RS Evans, *Electronic Health Records: Then, Now, and in the Future*, Yearbook Med. Inform., 2016; (Suppl 1): S48–S61. Published online 2016 May 20. doi: 10.15265/IYS-2016-s006.

segmentation for privacy" or DS4P tag described in 45 CFR 170.315(b)(7) and (b)(8). Other beneficial uses of metadata tags include:

- Determining the provenance of data to trace it back for data integrity, fraud investigations, etc. For example, it is through the metadata that forensic analysis can more specifically pinpoint who or when may health facts have been fraudulently changed.
- Enabling the development of a growing library of consensus-bundles of data, like the result of one lab test, that enable, in turn, more and more data to be made available to individuals through apps of their choosing when those apps use the Fast Health Interoperability Resource, or FHIR.
- Recognizing an authentic electronic credential of a user seeking their own data, so that they don't have to stop and sign a piece of paper to get their own PHI.

In 2000, OCR divided mostly unstructured data in the healthcare system into Protected Health Information, Summary Health Information, and Personally Identifiable Information. OCR then applied certain privacy and security processes specified in the relevant regulations to each of these broad buckets.

In 2019, we believe that to further advance crucial efforts to expand care coordination and allow health care to be effectively supplied through advanced digital tools and data science, OCR should consider revising the definition of PHI so that is accounts for the types of structured data in a more specific way than the 2000 broad categories did. Better distinction will support widespread interoperable exchange of standardized, structured, machine-readable health facts for care, personal care management, research and science, and population health.

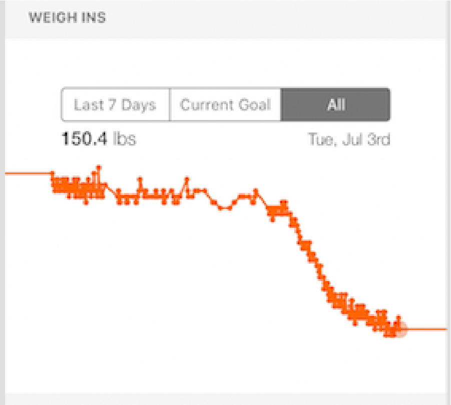
We also believe that modernized definitions would improve organizations' ability to provide individuals with access to their own data, and to provide appropriate accountings for disclosure of health facts subject to the Privacy Rule, as we discuss in greater detail below.

We recognize that revising the definition of PHI itself will require input from potentially thousands of interested parties and will require thoughtfulness, foresight, and care. Should OCR and HHS want to elicit more information on this topic, it might consider public listening sessions, so that all stakeholders can provide input in a way that more organically reflects the totality of input.

B. An Individual's Right to Access Their Own Health Facts (Questions 1-6)

At Omada, we succeed only when we engage our individual participants in our program. When individuals engage, they achieve the health outcomes for which Omada is paid. Therefore, unlike the much-decried fee-for-service health care system, it is in Omada's interest to robustly and consistently engage our individuals. We do that by continuously sharing data back to them in real-time about their successes, or about their particular needs for coaching on issues that are unique and specific to them.

It all starts with our digital scale, which is shipped to new participants already configured for their secure online account with us. The scale tells us instantly what the individual's weight is that day, but how they use that scale tells us instantly how the individual is using our program. And, for the participant, we curate and feed back to them in real-time what is happening to their weight as they participate in the program. Below is a screenshot of what one of our participants sees on their Omada app (this is from a real participant, used with their permission and de-identified to show you).



In response to Question 1, we have designed our program to feed some Core and Peripheral Health Facts back to individuals in real time. For health facts that an individual can obtain through our program or our app directly, there is no time delay.

For other health information that an individual wants but which is not available through our interface, our process is simple and rarely takes us more than two weeks to complete. Occasionally, however, we do use the full 30 days allotted by regulation. As a health care service provider with a predominantly digital infrastructure, we have very little paper and never require an individual to fill out a specific piece of paper in a specific way to get their own health facts. Nor do we ever require an individual to visit our office to request their health information. Times listed below are estimated averages, and individual requests may take more or less time.

In order:

1. The participant contacts us requesting health facts through our call center, through an email to our call center, or by messaging their coach who in turns forwards to our support staff. All three methods are handled by our call center support staff.
2. Within 2 business days, the support staff confirms the individual's identity with an outbound phone call. Our support staff also confirms the medium the individual wants, among the choices of PDF, paper, or an Excel file.
3. With the individual's preferences in mind, our support staff requests our data analytics team to extract, quality check and prepare the data. This process takes 3-8 business days, depending on load.
4. Typically within one more day, our support team then transmits it in an appropriate manner given the medium and where the individual requested we send the data.

5. If the request comes in from someone other than the individual, such as a physician's office or an attorney, and is presented to us on a HIPAA Authorization developed by the requestor, we confirm with the individual that they agree with the request, and proceed as above.

We recognize, however, that what individuals experience at Omada is the rare exception, not the norm. We believe that more health care stakeholders--even traditional ones like hospitals and physician practices-- could use digital technology and authentic digital identification methods more consistently. This would no doubt speed up and otherwise improve the experience for individuals. Modern methods that OCR and HHS might consider requiring through additional regulations include:

a. Requiring that covered entities that use certified EHRs (all of which now must include a patient portal) allow individuals to request their Core Health Facts using the portal's secure messaging system, for which the individual has already been issued identity credentials.
b. Through ONC's certification rule, requiring EHR developers to implement standard structured on-line forms, such as those developed by the American Health Information Management Association (AHIMA), as an EHR portal feature. This would enable individuals to more easily request both standard data sets, like a CCDA or an allergy list, and comprehensive data sets, like the records of a recent surgery, or radiology records.
c. Requiring that when a covered entity that does not use an EHR portal to allow individuals to request their own health facts, that covered entity must make its "paper form" for available for e-signature and submission through the portal, subject to identity proofing consistent with standards published by the National Institute for Standards and Technology (NIST), instead of making the individuals interact with a remote document processing location that may only accept faxes.
d. Financially penalize any covered entity that repeatedly fails to make health facts promptly available to individuals—OCR should not allow repeat offenders on this issue.
e. Strengthen and clarify the rule that state laws that make it harder for individuals to get their health facts are preempted by HIPAA.

As you can see from our practices, we are strong believers in an individual's right to obtain and use their own PHI. In 2018, we amended our program terms to confirm that every Omada participant owns the information they supply to us or that we collect about them with their permission.

Nevertheless, as we discussed above, we also think that should OCR update the definition of PHI to better account in the regulatory requirements for the actual data structures within digital health information today, to make it easier for organizations to ensure that individuals get their health information in a useful and accessible manner.

For example, If there are firm, clear regulatory distinctions between a Core Health Fact and a piece of Metadata, covered entities will be able to help individuals get more of the data to which individuals are entitled. An individual who wants lab values from a recent test will be able to choose the core health facts of lab values, but audit logs might not be necessary. More detailed definitions of the types of data also have the ability to improve efficiency by ensuring that resources are not wasted disclosing data that the individual actually does not want.

C. Sharing Data Between Covered Entities for Care Coordination (Questions 7-21)

As set forth above, Omada in many ways has built its business model--proving value and being paid for it--on the *existing* rules that permit but to not require a covered entity to share health facts with another covered entity. We have served over 200,000 individuals under this model. We have reported millions of health facts, such as the attainment of weight milestones or lesson completions, to payers and other providers who are covered entities. These covered entities in turn use this PHI for those organizations' care coordination, quality measurement or other legitimate health care operations. In our experience, the current rules do not impede care coordination.

As a health care provider that uses a sophisticated and modern digital platform to deliver our program, privacy, trust and security are fundamental. Without them, individuals will not trust us and will not engage with our program. Without privacy and security, employers and health plans will not pay for our health care services. Our participants and their payers trust us to share data only in the circumstances where they expect it and in compliance with applicable laws. Therefore, we think that the current rules are appropriate and should be maintained.

Switching it to disclosure-on-demand would undermine the trust inherent between a provider and an individual.

Having permission, however, does not mean the party disclosing should make it unreasonably difficult, slow, or expensive for another provider to get information they need for care of the same individual. In fact, we eagerly await open-specification Application Programming Interfaces to spread across the health care system so that we can interoperate with our participants' physicians as easily as we automatically collect their step data from trackers when they authorize us to do so. We use secure APIs daily both with customers who are covered entities and for internal processing of our data system, which is 100% cloud-based. We have plans in the near future to fully connect to health systems and their electronic health records so that our participants' providers can have easy access to program results. We do this in the interest of also accessing other health facts which would improve the effectiveness of our programs, like active prescriptions and lab results. To date, we have not done that due to the prohibitive cost of proving ourselves legitimate and obtaining permission to operate within some EHR vendor's ecosystems. We very much look forward to the day when API specifications are open for our developers to take advantage of. Therefore, we look forward to further opportunities to comment on this when we have had a chance to fully review ONC's forthcoming Notice of Proposed Rulemaking On Information Blocking.

We also think that were OCR to revise the definition of PHI to distinguish between Core Health Facts and Metadata or other elements of data as discussed above, OCR would be better able to describe what constitutes prompt, useful, and appropriate sharing using APIs and APPs between covered entities and when barriers to that constitute "information blocking."

Finally, OCR should accelerate and publish more interpretive guidance to improve the speed and efficiency of permitted (but not required) data sharing as follows:

1. OCR could develop, and then require, covered entities to use a standard form to request disclosure from each other. Once developed, a standard form could be made electronic, be e-signed, and built into electronic workflows. Such a standard form would, by necessity, have to rely on nationwide identity proofing standards ensure that use of a nationwide federally-developed form was not undermined by the idiosyncrasies of state signature laws, and would have to ensure that the party disclosing health information could rely on the HIPAA *bona fides* of the requester.
2. As discussed above, we use the existing rule at 45 CFR 16.506(c) as a fundamental part of our business model. However, we know that many healthcare technology companies fear expensive investigations and breach reporting if they in good faith try to share health facts with another covered entity for care coordination. Accordingly, OCR should consider eliciting more facts on the scope of this problem, potentially through public listening sessions. Based on the information elicited, if appropriate, OCR could consider adding to 164.506(c) or the Security Rule (as appropriate) a provision that a good faith attempt to share for care coordination, appropriately and securely transmitted but mis-delivered through no fault of the actual disclosing covered entity, is not a reportable breach by the covered entity (even if it remains a security incident that requires post-mortem analysis and remediation).

Because we think it is right to continue the current construct where sharing for care coordination permitted but not required, we do not think that sharing for care coordination should be a condition of participation for Medicare or Medicaid.

Omada is not submitting comments on questions 22-26.

D. Accounting for Disclosure (Questions 27- -41)

We applaud OCR for making another attempt to define and refine what is required to provide an Accounting of Disclosures to an individual. We note at the outset that Omada does not presently use a certified EHR. Nevertheless, as a health care provider, we do get asked for accountings and have had three such requests since January 2017.

For each response, we validate the individual's identity and that they were a participant in our program, research the types of disclosures we have made and whether they are required to be reported, and respond back to the individual accordingly. While this work takes only 2-5 hours per person, we do use the entire 30 days allowed by regulation.

That said, reporting individual outcomes to payers is a fundamental aspect of our business model, and we report frequently and in detail to relevant and appropriate payers, typically on a monthly basis for their population covered by Omada. Having served over 200,000 people to date, with hundreds of covered entity customers, we cannot estimate that number of disclosures. It is because of this outcomes-based model that we take the full 30 days to confirm that a person is our participant and how and to whom we have reported PHI before answering a request.

We do not allow our business associates to respond to request for accounting for us, and all disclosures of PHI are made based on decisions by Omada alone.

As Omada does not have an electronic health records system, we will not be responding to questions 35-41 directly. However, given our own data systems, and our recommendations in section II.A, above, we wanted to briefly comment on how better distinctions among the types of data would enable OCR to develop a more workable Accounting of Disclosures rule that is consistent with the individual's right to know AND with how modern data systems function.

The Accounting of Disclosures rule enables individuals to track who has seen or accessed or received their PHI so they can police the integrity, confidentiality and security of their very identity. Better separating Core Health facts from Metadata or audit logs will help OCR develop an Accounting of Disclosure rule for EHRS that does not result in the individual receiving reams of paper with one line of audit log and no obvious health facts. For example, clearly delineating among the different kinds of structured data will help OCR more easily develop a workable standard built around misuse or disclosure of core health facts, not audit logs or activity to correct bugs in Metadata Tags.

Privacy advocates that we are, we also believe that the identity of a covered entity's workforce members who have accessed, used or receive PHI should be disclosed only by court order, which is perfectly sufficient if criminal charges are pending or if a civil lawsuit about a breach of privacy is pending.

E. As HIPAA Evolves It Must Move Towards or Converge On Other Digital Information Privacy Standards

Since 2011, Omada has worked to establish personalized health care services using the latest digital tools. We connect our human coaches to individuals via secure messaging backed by data-science and population-wide analytics. Infrastructure like this is the next evolution of health care. One of the biggest themes throughout this eight year period is that more and more of the agencies that oversee or set standards for the health care system are becoming familiar with how the advent of 21st Century digital technology changes, and does not change, health care. We also observe that more and more of these agencies are interested in issues parallel to those of traditional concern to OCR, including:

Agency	Interests
Food & Drug Administration	○ Cybersecurity of devices ○ Privacy of data within Software as a Medical Device ○ Data integrity of software development (manufacturing processes)
HHS Office of the Inspector General	○ Digital record keeping and data integrity ○ Interoperability of data among health care stakeholders and individuals operating according to regulatory standards
Center for Medicare & Medicaid Services	○ Cybersecurity collaboration across the health care sector ○ Financially rewarding provider for patient engagement through access to the patient's own PHI
Federal Trade Commission	○ Privacy of health information collected outside HIPAA ○ Fair information security practices, even of HIPAA covered entities, as in LabMD vs. FTC
National Institute of Standards & Technology (NIST)	○ Privacy of health information technology ○ Security of health information technology
Federal Communications Commission	○ Privacy of health data transmitted via broadband license holders, whether within HIPAA or not.

Yet, to the outside observer, the rules and requirements remain as divergent as ever.

We are reiterating in this RFI comments that we made to FDA, as follows: In order for the U. S. health care system and the individuals, providers, and payers that constitute it to truly realize the benefits of digital technology, data science, and the power of big data, relevant agencies (and the above is just a small list) must redouble their efforts to coordinate and reach convergence on appropriate standards and expected business practices. Doing so sooner rather than later will:

1. Build trust by ensuring that consumer's information about their health is adequately, or even identically, private and secure, wherever it is collected and used.

2. Improve interoperability and appropriate information sharing for care coordination, population health, or scientific discoveries.
3. Improve efficiency by reducing wastefully overlapping compliance programs that are philosophically redundant but diverse in their details.

III. Conclusion

Omada has built its business as the nation's largest CDC-recognized provider of DPP health care services using the current HIPAA data sharing rules as a foundational element of our business model. We do not see a need to change that particular aspect of HIPAA.

We do, however, recognize that across the health care information spectrum, from FDA devices to HIPAA covered entities, to direct-to-consumer services and apps, the complex regulatory landscape is hindering innovation and eroding trust. It also is likely putting a chill on whatever data sharing for care coordination HIPAA allows, as data holders hesitate to share for fear of violating some other law that they have conflated with HIPAA.

To support continued innovation in health care delivery and strengthen consumer trust in an age where almost all data about a person can be directly or implicitly connected to health, we urge OCR to work with all stakeholders and agencies to ensure that any changes to the Privacy, Security or Breach Notification Rules move the regulatory environment closer to convergence, not farther away from it.

Respectfully submitted,

Sean Duffy, CEO

Lucia C Savage

Lucia C. Savage
Chief Privacy & Regulatory Officer