Regulatory De-Arbitrage in Twenty-First Century Cures Act's Health Information Regulation

Craig Konnoth[*]

INTRODUCTION

Health data regulation can be thought of at two levels. First, the micro-level of regulation has to do with Electronic Health Records (EHRs). Second, the macro-level concerns the networks on which EHRs are transmitted. The micro- and macro-levels of regulation interact. For example, EHRs need to be configured so that they can be transmitted on mandated networks. As a result, the lines do sometimes blur.

That said, the 21st Century Cures Act (Cures) clearly takes a dual approach to regulation.[1] Cures was passed in December 2016 on a bipartisan basis.[2] Its mandate was to address health data regulation at both the micro- and macro-levels.[3] At the micro-level, Cures seeks to address the problem of information blocking. It seeks to configure EHRs such that their users are incentivized to share the information to the greatest degree possible.[4] As I describe below, most penalties, however, apply only with respect to those who participate in the voluntary EHR certification program of the Office of the National Coordinator for Health Information Technology (ONC).[5] At the macro-level, Cures seeks to promote the creation of a national health information network (NHIN).[6] Like the certification program, participation in the network is voluntary.[7]

To the extent much of Cures' regulation relies on voluntary programs, regulatory arbitrage is easy. Firms can just choose not to participate in more

---

[*] Craig Konnoth is an Associate Professor of Law at the University of Colorado Boulder Law School.

[1] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, 1033 (2016) (codified as amended at 42 U.S.C. § 201 (2016)).

[2] Robert Pear, *Cures Act Gains Bipartisan Support That Eluded Obama Health Law*, N.Y. TIMES (Dec. 8, 2019), https://www.nytimes.com/2016/12/08/us/politics/cures-act-health-care-congress.html.

[3] *Id*. (illustrating the difference in the size of Cures Act compared to the Affordable Care Act, while stating both acts "affect every facet of medicine – from insurance coverage to delivery of care").

[4] *See* 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, 1176 (2016) (codified as amended at 42 U.S.C. § 300jj-52 (2016)).

[5] *Id*. at § 300jj-52(b).

[6] *See id.* at § 300jj-19(a) (describing the process of awarding grants to entities to support the collection of health information to be reported in accordance with this statute).

[7] *Id*. at § 300jj- 19(c).

robust regulation. However, in promulgating regulations, the Department of Health and Human Services (HHS) has taken steps to incent providers and other healthcare entities to participate both in the certification program and in the national network.[8] I conclude that while the incentives for participation in the certification program will be effective, those for participating in the national network are less so. I make recommendations to make such participation highly desirable.

Part I offers a brief history of health data regulation. Part II offers an overview of Cures. Part III explains Cures information blocking rules, and the incentivized voluntary approach it has adopted there. Part IV explains steps ONC has taken with respect to creating a national network, and the shortcomings to the voluntary approach there. Part V offers a solution.

I. THE HISTORY OF HEALTH DATA REGULATION

Health data regulation by Congress is now entering its second decade. While President George W. Bush issued an Executive Order founding the Office of the National Coordinator for Health Information Technology (ONC-HIT) in 2004,[9] it was only in 2009 that Congress entered the fray, passing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as part of the American Recovery and Reinvestment Act.[10] At the micro-level, HITECH focused on creating usable Electronic Health Records (EHRs).[11] HHS, at HITECH's behest, developed a voluntary certification program.[12] ONC developed criteria that any EHR had to meet in order to obtain ONC's imprimatur, or certification, that the EHRs was usable in various ways.[13] ONC largely devolved the task of certification to private

---

[8] *See* Medicare and Medicaid Programs; Electronic Health Record Incentive Program – Stage 3 and Modifications to Meaningful Use in 2015 Through 2017, 80 Fed. Reg. 62761, 62768 (Oct. 16, 2015) (to be codified at 42 C.F.R. pt. 412 and 495) (noting "Medicaid Eps and eligible hospitals demonstrating meaningful use for the first time in the Medicaid EHR Incentive Program would be required to attend for an her reporting period of any continuous 9-day period in the calendar year for purposes of receiving an incentive, as well as avoiding the payment adjustment under the Medicare Program.").

[9] *See* Nicolas Terry, *Meaningful Adoption: What We Know or Think We Know about the Financing, Effectiveness, Quality, and Safety of Electronic Medical Records*, 34 J. LEGAL MED. 7, 10 (2013) (explaining that the political history of EMRs began with President G.W. Bush in 2004).

[10] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (codified at 42 U.S.C. §201); *See generally,* Lucia Savage et al., *Digital Health Data and Information Sharing: A New Frontier for Health Care Competition?*, 82 ANTITRUST L. J. 593, 599 (2019) (explaining further that the passing of the HITECH Act provided over $36 billion in incentive payments for doctors and hospitals).

[11] *See* HIPAA Administrative Simplification; Enforcement, 74 Fed. Reg. 56123, 56124 (Oct. 30, 2009) (to be codified at 45 C.F.R. pt. 160) (stating "[t]he HITECH Act was incorporated into ARRA to promote the adoption and meaningful use of health information technology.").

[12] *See id*. at 56130. (noting "HHS expects a covered entity's voluntary compliance . . . .").

[13] *See* American Recovery and Reinvestment Act of 2009, Pub, L. No. 111-5, 123 Stat. 115

entities;[14] and in turn, published certification standards annually, subject to notice and comment.[15] At the macro level, the Act provided nearly $36 billion to distribute to eligible providers in public insurance programs that demonstrated "meaningful use" of EHR technology.[16] Such standards required providers to actually transmit data to other providers, clinical data registries, and the like, with more granularity over time.[17] HITECH proved effective at increasing uptake of EHRs.[18]

Despite this success, HHS's data interchange regulations were limited.[19] As a result, while participants could send certain clinical measures, few providers could actually share EHRs in a meaningful way with other providers or integrate EHRs received from others into their own systems.[20]

Further, private entities lacked incentives to exchange health records, and indeed, seek to block information interchange.[21] As a 2017 ONC Report

---

(2009) (codified at 42 U.S.C. §300jj-12) (providing specific areas for standardization, implementation of specifications, and criteria for certification).

[14] *See generally* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *Certification FAQ's*, HEALTHIT.GOV (Sept. 24, 2018), https://www.healthit.gov/topic/certification-ehrs/certification-faqs (explaining that developers and venders wishing to certify must first contact an ONC-Authorized Testing Laboratory to have their product tested, once tested and deemed to satisfy applicable certification criteria, the developer or vender then contacts an ONC-Authorized Certification bodies).

[15] OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH*, 2015 Edition Health IT Certification Criteria*, HEALTHIT.GOV (Jan. 24, 2018) https://www.healthit.gov/topic/certification-ehrs/2015-edition.

[16] *See generally* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH, *Meaningful Use and MACRA*, HEALTHIT.GOV (Feb. 12, 2019) https://www.healthit.gov/topic/meaningful-use-and-macra/meaningful-use-and-macra (noting the current CMS program that encourages health IT adoption is the Medicare Access and CHIP Reauthorization Act (MACRA)).

[17] *See* Medicare and Medicaid Programs; Electronic Health Record Incentive Program – Stage 3 and Modifications to Meaningful Use in 2015 Through 2017, 80 Fed. Reg. 62761, 62818 (Oct. 16, 2015) (to be codified at 42 C.F.R. pt. 412 and 495) (requiring the reporting of patients with a certain condition or all patients of a clinical or demographic group by participating providers); *See generally Clinical Quality Measures Basics*, CMS.GOV (Jun. 17,2019),https://www.cms.gov/RegulationsandGuidance/Legislation/EHRIncentivePrograms/ClinicalQualityMeasures.html (noting Medicare Promoting Interoperability Program Requirements for 2019).

[18] SHARONA HOFFMAN, ELECTRONIC HEALTH RECORDS AND MEDICAL BIG DATA 44 (Cambridge University Press, 2016); Julia Adler-Milstein & Ashish Jha, *HITECH Act Drove Large Gains in Hospital Electronic Health Record Adoption*, 36 HEALTH AFF. 1416, 1420 (2017).

[19] *See, e.g.,* Hoffman, *supra* note 18, at 55; *see also* Savage et al., *Digital Health Data and Information Sharing: A New Frontier for Health Care Competition?*, 82 ANTITRUST L. J. 594, 612 (2019) (noting that "Congress has noticed that health information is not flowing freely among health care providers.").

[20] A. Jay Holmgren et al., *Progress in Interoperability: Measuring US Hospitals' Engagement in Sharing Patient Data*, 36 HEALTH AFF. 1820, 1824–25 (2017).

[21] OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., DEP'T OF HEALTH AND HUMAN SERVICES: 2015 REPORT TO CONGRESS ON INFORMATION BLOCKING, 1,16 (2015) [hereinafter 2015 REPORT]; *See* Holmgren, *supra* note 20, at 1825–26 (explaining further that progress toward interoperability has been slower than projected).

noted, health IT manufacturers, health information exchange organizations (HIEs), hospitals, and even individual providers, engage in blocking "to control referrals and enhance their market dominance."[22] Burdening the ability to transmit information with another EHR, or enabling communication with another HIE allows EHR companies and HIEs to fight for market share, a "buy my product if you want to exchange information" mentality.[23] Similarly, preventing transmission of an individual's data to other providers will limit the ability of individuals to shop around for other doctors.[24] Thus, as health IT expert Professor Julia Adler-Milstein testified before the Senate, "EHR vendors do not have a business case for seamless, affordable interoperability across vendor platforms, and provider organizations find it an expense that they often can't justify."[25]

Blocking is quite prevalent and creates significant burdens on the health system. Last February, for example, the Physician Clinical Registry Coalition reported how specific EHR vendors, including EPIC, Allscripts, Cerner and Athena, charged exorbitant fees, imposed technical barriers and otherwise steered providers toward specific products through blocking.[26] As a quantitative matter, an exhaustive 2016 study showed that hospitals which used a specific regional market's dominant EHR vendor could engage in a greater degree of health data exchange than those using the non-dominant EHR.[27] The authors concluded that "dominant vendors in competitive markets may be least likely to facilitate HIE with other vendors."[28]

---

[22] *See* 2015 REPORT, *supra* note 21 at 16 (noting that healthcare providers have also been accused of information blocking, a common charge being to control referrals and enhance their market dominance).

[23] *See id*. at 15 (explaining that most anecdotal evidence regarding information blocking is directed at health IT developers charging fees that make sharing information cost-prohibitive for consumers and physicians).

[24] *Id*. at 16.

[25] *America's Health IT Transformation: Translating the Promise of Electronic Health Records Into Better Care: Hearing on Before the S. Comm. on Health, Education, Labor and Pensions*, (2015) (statement of Julia Adler-Milstein, Assistant Professor, Univ. of Mich.).

[26] Letter from Physician Clinical Registry Coalition to James A. Cannatti, Senior Counselor for Health Information Technology, Office of Inspector General, U.S. DEP'T HEALTH & HUM. SERV., & Kathryn Marchesini, Chief Privacy Officer, Office of the National Coordinator for Health Information Technology, U.S. DEP'T HEALTH & HUM. SERV., (Feb. 8, 2018), https://www.sts.org/sites/default/files/documents/020818_PCRC-Letter-Information-Blocking-EHR-Vendors.pdf; Joseph Conn, *ONC fail: EHR 'data blocking' still rampant*, MOD. HEALTHCARE (Apr. 17, 2015, 1:00 AM), https://www.modernhealthcare.com/article/20150417/NEWS/304179976/onc-fail-ehr-data-blocking-still-rampant.

[27] Jordan Everson & Julia Adler-Milstein, *Engagement In Hospital Health Information Exchange Is Associated With Vendor Marketplace Dominance*, 35 HEALTH AFF. 1286, 1286 (2016).

[28] *Id.* at 1292.

II. HEALTH INFORMATION REGULATION IN THE CURES ACT

Information blocking harmed health data regulation at both the micro-level by making EHRs harder to use and at the macro-level by making it harder to create a national data network. Enter Cures. Section 4002 of Cures prohibits developers of EHRs that participate in ONC's certification program from taking "any action that constitutes information blocking."[29] Further, the developer is prohibited from restricting users from communicating about "the usability . . . interoperability . . . security," of the EHR, their "experiences when using" the EHR, "the manner" of their use, and the "business practices of developers."[30] In a later less prominent, subsection, Cures requires that Certified EHR technology (CEHRT) must also make available information regarding "application programming interfaces" (APIs).[31] APIs are interfaces that could link with apps from, say, an iPhone, allowing a user to download patient data from an EHR.[32] This helps promote data sharing.

Section 4002 works hand in glove with Section 4004, which prohibits information blocking.[33] Information blocking is defined as "a practice that … is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information."[34] If a developer engages in information blocking or should know a practice may result in information blocking, a constructive knowledge standard subjects the developer to penalties.[35] Providers must have actual knowledge to be held liable.[36] Both providers and developers are subject to penalties for blocking.[37] Developers face up to $1 million per violation; provider penalties are determined by rulemaking.[38] Finally, the statute permits blocking in some instances, the determination of which is completely in the hands of HHS.[39]

Lastly, Section 4003 seeks to develop a national network. It mandates that ONC "shall convene appropriate public and private stakeholders to develop or support a trusted exchange framework for trust policies and practices and for a common agreement for exchange between health information

---

[29] Genevieve Morris & Elise Sweeny Anthony, *21st Century Cures Act Overview for States*, OFFICE NAT'L COORDINATOR FOR HEALTH INFO. TECH., at 7 (Jan. 8, 2018), https://www.healthit.gov/sites/default/files/curesactlearningsession_1_v6_10818.pdf.
[30] 21st Century Cures Act, Pub. L. No. 114-255, §4002, 130 Stat. 1033, 1159–60 (2016).
[31] *Id.* at 1160.
[32] THE OFFICE OF THE NAT'L. COORDINATOR FOR HEALTH INFO. TECH., ABOUT APIS, at 2, https://www.healthit.gov/api-education-module/story_content/external_files/hhs_transcript_module.pdf (last visited Nov. 24, 2019).
[33] 21st Century Cures Act § 4004, 130 Stat. at 1176.
[34] *Id.* at 1176.
[35] Morris & Sweeny Anthony, *supra* note 29, at 31-32.
[36] *Id.* at 31.
[37] *Id.* at 32.
[38] 21st Century Cures Act § 3022(B)(2)(A), 130 Stat. at 1178.
[39] Morris & Sweeny Anthony, *supra* note 29, at 31.

networks."[40] This agreement will determine "a common method for authenticating trusted health information network participants; … a common set of rules [and] … organizational and operational policies … and a process for filing and adjudicating noncompliance with the terms of the common agreement."[41]

III. MICRO-LEVEL RULES REGARDING EHRS

This Section provides an overview of the EHR regulation emerging from Cures. It also explains how ONC provides incentives for entities to assume more onerous regulation.

In laying on the requirements for EHRs, ONC engages in what I term elsewhere "concentric regulation." By this, I mean that different sets of regulatees are subject to an escalating set of requirements. First, at the outer edge are providers. All providers and certified developers are subject to the information blocking rules.[42] Notably, although the statute permits HHS to forbid any developer—not just certified developers—from engaging in information blocking, the regulations do not reach that far.[43] These rules set the minimum set of requirements, prohibiting providers from knowingly engaging in behavior that is unreasonable and would "interfere with…access, exchange, or use of electronic health information."[44] Per the statute, ONC set out a list of exceptions that permitted providers to withhold information. These comprise: (1) "preventing harm"; (2) "promoting . . . privacy"; (3) "promoting . . . security"; (4) "recovering costs"; (5) situations where the "requests . . . are infeasible"; (6) "licensing of interoperability elements on reasonable and non-discriminatory terms"; and (7) systems maintenance.[45]

Preventing information blocking is, of course, the basic minimum required to promote interoperability. The rule also takes affirmative steps to promote interoperability and functionality.[46] This second level requirement did not apply universally—rather it applied only to a limited set of EHRs—so-called Certified Electronic Health Record Technology (CEHRT), and by extension, to the limited set of providers that used it.[47]

There are three features of the heightened set of CEHRT requirements that

---

[40] 21st Century Cures Act § 4033(b)(9)(B)(i), 130 Stat. at 1165.
[41] *Id.* at 1165-66.
[42] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 42, 7424 (Mar. 4, 2019) (to be codified at 45 C.F.R. pt. 170-71) [hereinafter 21st Century Cures Act].
[43] *Id.*
[44] *Id.* (noting that CEHRT are subject to the same requirements but have a constructive knowledge standard).
[45] *Id.* at 7602-05.
[46] *Id.* at 7485.
[47] *Id.* at 7495 (noting that second level requirement does not technically apply to CEHRT users certified only to a CDS functionality).

bear mentioning. First, there is greater functionality. CEHRT must comply with a new data set developed by ONC in consultation with stakeholders.[48] This U.S. Core Data for Interoperability set (USCDI) was initially only used as part of ONC's HITECH incentive program, but now, ONC hopes, will be extended to all EHRs.[49] Finally, ONC proposes to heighten opioid functionality in CEHRT, and issued a detailed set of explanations on that front.[50] Additionally, and relatedly, CEHRT will have to be able to provide greater support for electronic prescribing than before, including providing information about risk mitigation strategies.[51]

The second aspect of CEHRT certification sought to promote interoperability. Per the statute, the rule required CEHRT developers to provide assurances that they did not engage in information blocking, and did not restrict the usability, interoperability, security, experiential, and business practices related information, as the statute required.[52] This effectively nullified so-called "gag clauses" that developers inserted into contracts with providers, that prevented the latter from communicating problems about the EHRs.[53] Finally, and perhaps most innovatively, the rule built on the glancing reference on APIs in the statute. As the Act required, the rule provides that "health information from such technology" must "be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law."[54] The Cures Act's API Condition of Certification also states that a developer must, through an API, "provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws."[55] At the population level, the goal is to ultimately promote Clinical Decision Support (CDS) to a greater degree than ever before, allowing a multitude of researchers to access and use the data in new and innovative ways.[56]

The third set of requirements concerns assurances as to CEHRT functionality. ONC promotes real world testing, requires developers to publish testing plans, and the results of tests.[57] Indeed, ONC has requested comments on the idea that CEHRT developers *must* participate in the national Trusted Exchange Framework & Common Agreement (TEFCA) network in order to prove that their product meets certification standards.[58] Further,

---

[48] *Id.* at 7495.
[49] *Id.* at 7439-40
[50] *Id.* at 7461-65.
[51] *Id.* at 7444-45.
[52] *Id.* at 7593.
[53] *Id.* at 7476.
[54] *Id.* at 7594.
[55] *Id* . at 7476.
[56] *Id.* at 7605.
[57] *Id.* at 7496.
[58] *Id.* at 7466.

CEHRT developers must submit attestations that their products are up to snuff every six months.[59] ONC seeks to make compliance easy—indeed, if a CEHRT developer cannot certify that they are in compliance, they can indicate as much to ONC.[60] ONC is willing to work with such a developer.[61] Further, customers can make complaints. They should first try to resolve the complaint with the developer, then contact the private certification body.[62] But if those steps do not work, they can go to ONC.[63] If ONC does not find the entity cooperative, ONC will take various steps including suspending, or terminating certification of future, and if necessary, current, products, as well as publicly shame the offender by listing them publicly.[64] ONC can also refer and work in tandem with the OIG.[65]

These three sets of second level requirements are more onerous than simply the information blocking requirements at the first level. At the same time, they are voluntary—a developer might simply decline to obtain certification. However, they are also highly desirable. The nation's health system would greatly benefit from EHRs with a high degree of opioid related, privacy supportive, functionality, that all use the same data sets, and that support apps. How does ONC incent voluntary certification?

The structure of rules supports voluntary certification by imposing information blocking liability on providers. While the statute provides that providers are only liable if they knowingly engage in information blocking, to ensure that they do not face liability or investigation, a rational provider is more likely to seek EHRs that do not engage in information blocking. This, by itself, might cause non-certified EHRs to comply with the EHR information blocking requirements, even though the regulations do not require them to do so. A non-certified EHR that continues to engage in information blocking might soon find itself without a customer base.

But the more important point is—how is the provider to *know* whether an EHR engages in information blocking or not? ONC and OIG have declined to engage in *any* oversight of non-certified EHRs even though the statute authorizes some such oversight.[66] On the other hand, CEHRT publishes test results, might participate in TEFCA, is subject to a complaint mechanism, and provides attestations twice a year.[67] The rules authorize OIG to investigate only CEHRT developers (though the statute is written more

---

[59] *Id* at 7501.
[60] *Id.* at 7502
[61] *Id.*
[62] *Id.* at 7503.
[63] *Id* at 7503.
[64] *Id.* at 7504-06.
[65] *Id.* at 7507.
[66] *Id.* at 7502-07.
[67] *Id.* at 7466, 7496, 7501, 7503.

broadly).[68] A rational provider would be more likely to pick a CEHRT that is subject to these oversight mechanisms. The provider can investigate certifications, complaint history, and past corrective actions to choose the right EHR that would insulate themselves from future liability in any situation in which information blocking occurs. This, in turn, incentivizes EHRs to obtain certification—in order to obtain access to a larger customer base.

In this way, ONC discourages regulatory arbitrage. A developer *could* choose to forego certification—but ONC has arranged market conditions such that that option would be undesirable. Thus, ONC has encouraged voluntary adoption of higher requirements.

IV. MACRO LEVEL REGULATION—TEFCA

Pursuant to the instructions in Cures, in January 2018, HHS published a draft TEFCA.[69] That draft was subject to commentary, and in April 2019, TEFCA released another draft.[70] According to the most recent draft, "[t]he TEF and the Common Agreement will be distinct components that together aim to create technical and legal requirements for sharing EHI [electronic health information] at a nationwide scale across disparate HINs [health information networks]."[71] As ONC explains, "[t]he TEF describes a common set of principles that facilitate trust between HINs.[72] These principles serve as 'rules of the road' for nationwide electronic health information exchange."[73] ONC will develop the TEF.[74] On the other hand, "[t]he Common Agreement will provide the governance necessary [for] a functioning system of connected HINs . . . The architecture will follow a 'network of networks' structure, which allows for multiple points of entry and is inclusive of many different types of health care entities."[75] Nonetheless, as I suggest above, TEFCA's data management requirements, both on the privacy and security front, are likely to be detailed and robust.

As with the previous draft, however, the national networks will be unified under the supervision of "a single, industry-based [Recognized Coordinating Entity (RCE)]."[76] This RCE will "onboard[] organizations to the final

---

[68] *Id.* at 7507.
[69] OFF. OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., DRAFT TRUSTED EXCHANGE FRAMEWORK (2018) [hereinafter DRAFT].
[70] OFF. OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., TRUSTED EXCHANGE FRAMEWORK AND COMMON AGREEMENT DRAFT 2 (2019) [hereinafter DRAFT 2].
[71] *Id.* at 4.
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] DRAFT, *supra* note 69, at 30. Accordingly, I do not agree with the comment from the American College of Surgeons that purports to find ambiguity in the term "industry-based",

TEFCA, ensur[e] Qualified [networks] comply with the terms and conditions of the TEFCA, address[] non-conformities . . . , develop[] additional use cases," and engage in "day-to-day management and oversight of unaffiliated Qualified [health information networks]."[77] The RCE will *itself* have the power to "update[e] the TEFCA over time . . . ."[78] Under the RCE will be 7 large entities who will each run regional qualified health information networks (QHINs).[79]

The TEF seeks to promote various methods of information interchange. Targeted queries allow one QHIN to seek EHI from another specific QHIN.[80] A broadcast query allows the QHIN to query all other QHINs.[81] Finally, a QHIN can also "push" data to another QHIN even if it is not in response to a query.[82] TEFCA provisions address "meaningful choice, written privacy summaries, data integrity, identity proofing, access control, user authentication, and auditing consistent with industry best practices," which often exceed those required by existing law.[83] The TEF critically mandates "[c]ollaborat[ion] with stakeholders across the continuum of care to exchange EHI, even when a stakeholder may be a business competitor."[84] This would preclude, for example, "throttling the speed with which data is exchanged purely for competitive reasons, limiting the data elements that are exchanged with healthcare organizations that may be their competitor or a competitor of one of their participants, or by requiring burdensome testing requirements designed to unfairly deter or discourage connections that do not benefit the HIN"—all practices which entities have been known to engage in with competitors.[85] It seeks to promote access by other caregivers and even exchange of population level data for research.[86]

Participation in TEFCA is voluntary.[87] The requirements of TEFCA exceed the requirements of existing regulation—for example, industry standards of privacy and security may exceed those mandated by HIPAA and

---

as the language of TEFCA forecloses that interpretation); TEFCA COMMENTS, at 809 (arguing (The American College of Surgeons) that the term "is broad and open to interpretation" and that it could be "a quasi-government entity").

[77] *Id.* at 9.

[78] *Id.* (noting that additionally, instead of one firm, it would consider giving the contract to an organization created by a group of firms).

[79] *Id.* at 5.

[80] DRAFT 2, supra note 70 at 13.

[81] *Id.*

[82] *Id.*

[83] *Id.* at 16.

[84] *Id.* at 24.

[85] *Id.* at 27; s*ee also id.* at 47-48 (detailing Cooperation and Non-Discrimination sections).

[86] *Id.* at 24.

[87] Rebecca Pifer, *Industry interoperability concerns plague TEFCA draft*, HEALTHCARE DIVE (June 20, 2019), https://www.healthcaredive.com/news/industry-interoperability-concerns-plague-tefca-draft/557208/.

state regulation.[88] However, I believe it is fair to say that the additional regulatory burden does not, at first, seem much greater than that already imposed by current law on all healthcare entities.

However, the new TEFCA draft overlooks a set of comments from the previous draft that explained that TEFCA would create regulatory burdens because of the patchwork of state privacy laws.[89] With one or two exceptions, every commenter to address the issue, from states to private entities, has rejected the approach that TEFCA currently takes, that varies applicable privacy policy state by state.[90] As the Florida state agency notes, this would lead to the precise fragmentation that TEFCA was meant to avoid.[91] Similarly, as the American Hospital Association notes, "it will be very challenging, if not impossible to know whether responding to a specific request is, in fact, allowed by applicable law," given the multiple laws across the country.[92] Thus, commenters suggest they would not join the network if they had to comply with a patchwork of state privacy law.[93]

Thus, even as private industry celebrated TEFCA's voluntary approach,[94] others criticized it. As the Louisiana state exchange explained,

---

[88] DRAFT, *supra* note 69, at 38 (describing crosswalk between NIST and HIPAA standards).

[89] *See generally* DRAFT 2*, supra* note 70.

[90] The author has a pdf binder of all comments submitted on TFCA. The numbering reflects the Bates number on the pdf. TEFCA COMMENTS. "SHIEC strongly encourages ONC to provide the industry with guidance on addressing variation in state and federal laws related to privacy and consent. TEFCA is silent on how to address this variation, other than to state that all applicable law must be followed" and calling for "strong leadership to set a national approach." *Id.* at 684. "While the trusted exchange framework highlights the importance of privacy and consent as one of the core principles, the common agreement section of the document seems to pay little specific attention to the reality of inconsistent state, local and tribal patient consent and data sharing laws that are often an obstacle to cross-jurisdiction interoperability." *Id.* at 951. "GNYHA seeks additional detail on how ONC plans to harmonize varying state consent rules for health information exchange (For example, while some states do not require separate patient consent for exchanging patient information unless a patient opts out, others such as New York State require a patient to opt-in to the exchange. How will this be reconciled?), among others." *Id.* at 660.

[91] TEFCA COMMENTS, at 671 (stating "Variation in state law surrounding patient authorization remains a significant barrier to exchange. In Florida, this results in a strict inability to exchange with states who do not obtain explicit patient consent to exchange sensitive data. Laws that reach beyond the HIPAA requirements create a landscape where some states are virtual islands . . .").

[92] *Id.* at 61; *see also id.* at 781 (providing an example: "an out-of-state HIE seeking to obtain a patient's information from a New York State HIE would need to have that patient's consent in hand in order to access that information . . . even if the out-of-state HIE properly followed its own states opt-out rules for consent").

[93] *Id.* at 801.

[94] Letter from Ashley Thompson, Sen. VP AHA, to Don Rucker M.D., Nat'l Coord. Health Info. Tech., (June 17, 2019); TEFCA COMMENTS at 56 ("The AHA applauds ONC for pursuing a voluntary 'network of networks' approach . . ."); *Id.* at 852 ("We also agree with and appreciate the voluntary nature of the TEFCA.").

> Given that participation in the Trusted Exchange Framework is voluntary, it is unclear how it will achieve the Cures' determination that satisfy (1) complete access to health information without special effort; and (2) no information blocking. If a provider, payer or other organization that holds parts or the whole content of one's health information chooses not to participate in the TEFCA, that in itself would limit complete access to one's health information and may even constitute information blocking.[95]

Indeed, certain groups emphasize their need for autonomy.[96] As the American Medical Association, Connected Health, and others emphasized, not only should the government not mandate connection, but insurers should not be allowed to make providers join TEFCA as a condition of network participation.[97]

V. POSSIBLE INCENTIVES FOR JOINING TEFCA

Could ONC incentivize joining TEFCA as it seeks to incentivize participation in its certification program? I explain what the incentive should be, the shape it should take, and the process for implementing it.

A. Creating a TEFCA Incentive

ONC might consider offering various incentives for joining TEFCA. Rules that CMS developed in consultation with ONC might provide one set of incentives. In those rules, CMS required private entities working under the umbrella of Medicare and Medicaid (such as Medicare Advantage plans), as well as payers on federally funded exchanges to create APIs that are analogous to those required of CEHRT, to make data available for patients, and to engage in certain kinds of data exchange activities.[98] CMS proposes that participation in TEFCA would satisfy some of these data exchange activities.[99] This incentive, however, is limited to only a small set of plans.

Another approach might simply be to provide subsidies to entities joining TEFCA. Thus, as the Medical Group Management Association suggests, ONC could "[c]reat[e] appropriate financial incentives . . . including payment incentives and payment for e-consultation or incentives for use of HIN

---

[95] TEFCA COMMENTS *supra* note 90 at 395 (nursing professionals expressing similar concerns).
[96] *Id.*
[97] *Id*. at 133, 197.
[98] Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally Facilitated Exchanges and Health Care Providers, 84 Fed. Reg. 7610, 7616 (proposed Mar. 4, 2019) (to be codified at 45 C.F.R. pt. 170) [hereinafter Interoperability and Patient Access].
[99] *Id.* at 7618, 7642.