THE MILBANK QUARTERLY
A MULTIDISCIPLINARY JOURNAL OF POPULATION HEALTH AND HEALTH POLICY

Original Scholarship

Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles?

MICHELLE M. MELLO,[*,†] JULIA ADLER-MILSTEIN,[‡] KAREN L. DING,[*] and LUCIA SAVAGE[§]

[*]*Stanford Law School;* [†]*Stanford University School of Medicine;* [‡]*University of California, San Francisco;* [§]*Omada Health*

Policy Points:

- Historically, in addition to economic and technical hurdles, state and federal health information privacy laws have been cited as a significant obstacle to expanding electronic health information exchange (HIE) in the United States.
- Our review finds that over the past decade, several helpful developments have ameliorated the legal barriers to HIE, although variation in states' patient consent requirements remains a challenge.
- Today, health care providers' complaints about legal obstacles to HIE may be better understood as reflecting concerns about the economic and competitive risks of information sharing.

Context: Although the clinical benefits of exchanging patients' health information electronically across providers have long been recognized, participation in health information exchange (HIE) has lagged behind adoption of electronic health records. Barriers erected by federal and state health information privacy law have been cited as a leading reason for the slow progress. A comprehensive assessment of these issues has not been undertaken for nearly a decade, despite a number of salient legal developments.

Methods: Analysis of federal and state health information privacy statutes and regulations and secondary materials.

Findings: Although some legal barriers to HIE persist, many have been ameliorated—in some cases, simply through improved understanding of what the law actually requires. It is now clear that the Health Insurance Portability and Accountability Act presents no obstacles to electronically sharing

The Milbank Quarterly, Vol. 96, No. 1, 2018 (pp. 110-143)

protected health information for treatment purposes and does not hold providers who properly disclose information liable for privacy breaches by recipients. The failure of federal efforts to establish a unique patient identifier number does slow HIE by inhibiting optimal matching of patient records, but other action to facilitate matching will be taken under the 21st Century Cures Act. The Cures Act also creates the legal architecture to begin to combat "information blocking." Varying patient consent requirements under federal and state law are the most important remaining legal barrier to HIE progress. However, federal rules relating to disclosure of substance-abuse treatment information were recently liberalized, and development of a technical standard, Data Segmentation for Privacy, or DS4P, now permits sensitive data requiring special handling to be segmented within a patient's record. Even with these developments, state-law requirements for patient consent remain daunting to navigate.

Conclusions: Although patient consent requirements make HIE challenging, providers' expressed worries about legal barriers to participating in HIE likely primarily reflect concerns that are economically motivated. Lowering the cost of HIE or increasing financial incentives may boost provider participation more than further reducing legal barriers.

Keywords: legal, electronic health record, health information technology, health information exchange.

The 21st Century Cures Act, enacted by Congress in December 2016, devotes nearly a hundred pages to measures aimed at accelerating progress toward widespread interoperability of electronic health records (EHRs).[1] These provisions reflect an understanding that, alongside technical, economic, and workflow issues,[2-5] health information privacy laws are perceived as posing obstacles to the growth of electronic health information exchange (HIE) among health care providers. Despite efforts to craft federal privacy law so as to permit information sharing among providers for treatment purposes, finding the balance between allowing information to flow freely to improve health care and respecting patients' privacy rights has proved challenging.

In the mid-2000s, a flurry of scholarly articles called attention to the problem of legal barriers to HIE and plumbed its contours.[6-12] A decade on, where do things stand? Several developments over the past decade (Table 1) make it timely to reevaluate. We review the landscape, the likely effects of recent efforts to smooth the "legal speed bumps,"[6] and the prospects for HIE growth going forward. We focus on information exchange for clinical purposes, rather than public health or research uses.

Table 1. Key Developments Affecting the Continuing Relevance of Legal Barriers to Health Information Exchanges, 2007-2017

Development	Importance
Passage of 21st Century Cures Act (2016)	• Directs ONC to issue further guidance to address fears about HIPAA and other laws as barriers to HIE. • Directs HHS to convene stakeholders to determine how federal substance abuse confidentiality regulations affect patient care and privacy. • Directs HHS to issue a rule requiring that health information technology entities, as a condition of Medicare certification, do not engage in information blocking. Requires providers to attest they are not engaging in information blocking. Provides civil remedies for information blocking practices. • Directs GAO to study how to ensure accurate patient record matching. Convenes a committee to recommend standards to promote interoperability, including technology for accurate patient record matching. • Directs HHS to lead the development of a new strategy to promote interoperability, which could include new financial incentives.
Release of ONC/OCR fact sheets on HIPAA (2016)	• Clarifies that protected health information may be exchanged for treatment or health care operations purposes without patient authorization and that disclosing providers bear no liability for the acts of downstream data recipients.
Release of SAMHSA Final Rule on Confidentiality of Substance Abuse Disorder Patient Records (2017)	• Allows patients to give broader consent for disclosure of drugs- and alcohol-related information instead of naming specific recipients.
Integration of DS4P data segmentation standard into electronic health record software	• Allows providers to readily identify parts of a patient's electronic health record that are subject to heightened requirements for disclosure under state or federal law.
Development of road maps for harmonizing state law by Health Information Security and Privacy Collaboration (2007-2009) and National Governors Association (2016)	• Provides concrete guidance to states about how to harmonize state laws imposing different requirements for patient consent for disclosure of health information—or in the alternative, to create legally binding interstate agreements establishing which rules will govern. • Highlights examples of how states have modified their privacy laws to achieve greater consistency with HIPAA and advance HIE.
Amendment of state privacy laws to ease patient consent requirements	• Reduces inconsistency with HIPAA and other state laws, simplifying interstate HIE. • Reduces the prevalence of opt-in consent regimes, thereby increasing rates of patient participation in HIE.

Abbreviations: ONC = Office of the National Coordinator for Health Information Technology; HIPAA = Health Information Portability and Accountability Act; HHS = Department of Health and Human Services; GAO = Government Accountability Office; OCR = Office for Civil Rights; SAMHSA = Substance Abuse and Mental Health Services Administration; DS4P = Data Segmentation for Privacy initiative; HIE = health information exchange

We conclude that some important legal barriers persist, but many legal issues that health care providers have cited as obstacles to their participation in HIE are today quite tractable, or even illusory. Complaints about these issues may, to some extent, be understood as standing in for other concerns—namely, provider organizations' assessment that participating in HIE does not offer them sufficiently valuable benefits and could involve competitive harm.

The Slow Growth of HIE

HIE is the process of electronically sharing identifiable patient health information across provider organizations to support treatment and related needs, such as quality measurement and care coordination. HIE can occur at various levels of scale. Two organizations can establish HIE with each other, or HIE can be established in ways that enable exchange among a large set of providers, based on geographic location, a shared EHR vendor, strategic alignment, or some other boundary. HIE at a larger scale typically involves a third-party intermediary that establishes the technical infrastructure and governance approach. Although there are many types of information exchange arrangements,[13] they face similar legal barriers.

Information about progress toward HIE has arisen from studying third-party efforts to establish exchange organizations, which fall into three categories.[13] Community HIE efforts, often called "health information organizations" (HIOs) or regional health information organizations (RHIOs), involve "a neutral, third-party organization that facilitates information exchange between providers within a geographical area to achieve more effective and efficient healthcare."[14] There are more than 100 operational community HIEs, but they have experienced a high failure rate and report many barriers spanning legal, governance, technical, sustainability, and provider engagement.[15-19]

HIE initiatives by EHR vendors, the second category, have focused on connecting providers that use the same EHR vendor. For example, Epic operates a large vendor network, the Care Everywhere Network. This "walled-garden" HIE is available only to providers who are Epic members. The third category, enterprise HIE efforts, strategically aligns groups of providers by using HIE to encourage referrals and tighter organizational relationships. Compared to community HIE efforts,

there is less research available on the progress of the latter two types of initiatives.

A few HIE efforts do not fit in the above categories. One example is the eHealth Exchange, a large, national exchange framework that has been used by 4 federal agencies, about 50% of US hospitals, 26,000 medical groups, and 100 million patients in 50 states.[20] Originally a federal initiative, it was handed off to the private-sector Sequoia Project in 2012. eHealth Exchange's current incarnation, known as Carequality, is not a technical infrastructure for information transmission and storage, but rather a legal framework and means of credentialing exchange transactions of those who participate in it and pay fees.[21] A second example is the CommonWell Health Alliance, a private consortium that developed along similar lines, but without federal financial support.[22] Both organizations developed their own legally enforceable master agreements for their participants setting out expectations, what constitutes a breach, and where liability for breaches rests. In 2016, following congressional action on the slow pace of interoperability, Sequoia and CommonWell announced a collaboration.[23] In October 2017, the Office of the National Coordinator for Health Information Technology (ONC) deputy national coordinator testified before the Senate Committee on Health, Education, Labor and Pensions that Sequoia and CommonWell were collaborating with ONC to help it fulfill its obligations under the 21st Century Cures Act to develop a uniform, voluntary trust agreement.[24]

Varied approaches to HIE have emerged because of the long-recognized value of exchanging patients' health information electronically across providers coupled with the rapid adoption of EHRs over the past decade.[25] In concept, capturing patient health information electronically in EHRs should make sharing it easier. However, HIE has not proven easy, and participation in HIE has lagged behind adoption of EHRs.

While there are many ways to measure engagement in HIE, ONC's Interoperability Roadmap lays out 4 core domains: find, send, receive, and use.[26] According to the most recent national data (Table 2), only about half of hospitals and a third of office-based physicians reported finding patient health information electronically from sources outside their health system, and only a fifth of hospitals engaged in all 4 domains.[27,28] On another measure, the percentage of care transitions for which a summary care record was electronically sent to the subsequent provider, only

Table 2. Health Care Providers' Participation in Domains of Health Information Exchange, 2015[a]

Domain	Office-Based Physicians	Non-Federal Acute Care Hospitals
Find: Electronically find (query) patient health information from sources outside their health system	34%	52%
Send: Electronically send patient information to sources outside their health system	38%	85%
Receive: Electronically receive patient information from any providers outside their organization	38%	65%
Use: Can easily integrate (eg, without manual entry) health information received electronically into their EHR	31%	38%
All four of the above domains	Not available	21%

[a]Data from the Office of the National Coordinator for Health Information Technology (2016)[27] and Holmgren et al (2016).[28]

15% of eligible providers and 6% of eligible hospitals engaged in this practice for at least 80% of care transitions.[29]

The United States has essentially adopted a "bottom-up, evolutionary" approach to HIE rather than mandating participation.[30] An extraordinary amount of effort, however, has been put into spurring the growth of HIE with the ultimate goal of creating fully interoperable health records. Since 2004 there has been a federal office dedicated to the job: ONC, which sits within the Department of Health and Human Services (HHS). ONC has funded multiple state initiatives to plan and pursue activities to advance HIE.[31,32] In 2009, the Markle Foundation's Connecting for Health public-private collaborative completed several years of intense work, culminating in a set of standard contracts and policies that organizations interested in HIE could adopt.[33] With the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009,[34] ONC grew and was tasked with awarding hundreds of millions of dollars in grants as seed money for HIE. Prior to HITECH, a few states, notably New York,

had enacted statutory frameworks intended to encourage HIE. After HITECH, about half of states enacted legislation to take advantage of the available grants and in some cases provide additional incentives or legal and privacy frameworks for HIE.[35]

That such substantial time and resources have been devoted to promoting HIE without achieving broad success reveals the difficulty of the enterprise. Although there are many barriers to HIE participation, legal obstacles regularly emerge in discussions of why progress has been limited. In a recent national survey of community HIEs, 86% cited privacy and confidentiality concerns as a barrier to progress, 81% cited managing the complexity of patient consent, and 82% cited accurately linking patient records[36]—all problems traceable to laws or stakeholders' understanding of laws. For example, the United States lacks a unique patient identifier (UPI) for use in linking records because Congress has prohibited the use of federal funds for its development or implementation. When ONC and the Centers for Medicare and Medicaid Services (CMS) invited comments from stakeholders on a strategy for accelerated progress toward HIE, many expressed concerns about being able to comply with state and federal privacy laws, especially those regarding patient consent for information disclosure.[25]

We thus turn to an analysis of the most important perceived legal barriers to HIE, which are of 5 main types: (1) the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule; (2) varying state-law requirements concerning patient consent for record disclosure; (3) special federal- and state-law protections for particular types of sensitive health data; (4) the failure of attempts to implement a uniform patient identifier; and (5) insufficient measures to prevent "information blocking." We assess how formidable these legal barriers are and how this has changed over the past decade.

We focus on privacy-law issues because they have been at the forefront of discussions about HIE. Cybersecurity concerns, too, may have chilled interest in HIE in recent years. In May 2017, for instance, the WannaCry malware infected hundreds of hospital operating systems across Europe, holding electronic health information for ransom and causing shutdowns of care. Although hacking incidents may give rise to liability, they raise a quite different constellation of issues that is beyond the scope of this article.

HIPAA Privacy Rule

HIPAA, passed in 1996 and implemented over the next several years,[37,38] has been much derided as a clumsy vehicle for protecting the privacy of personal health information. When this information is held by certain types of health care organizations, such as hospitals and health plans, it is called *protected health information*, or PHI. Although the HIPAA statute's passage predated the implementation of HITECH, the legislation actually derived from Congress's decision to require that medical bills be digitized. That digitization necessitated the creation of privacy (and security) requirements, and the HIPAA Privacy Rule was born.

To this day, Privacy Rule requirements for collecting, maintaining, accessing, and disclosing PHI are the same whether the information is in paper or electronic form. (HIPAA's Security Rule, in contrast, applies solely to electronic health information.) HIPAA's architects thus anticipated electronic information exchange rather well, creating what has proven to be a workable framework for information transfer for clinical purposes. However, the statute was not designed with today's HIE in mind. Whenever a law must be applied to a novel set of facts, the potential for misapprehensions arises. Indeed, persistent, widespread misconceptions among providers about how HIPAA's requirements apply to electronic exchange of a wide range of clinical data have provoked anxiety about liability, impeding HIE.

The Privacy Rule generally requires written patient authorization for release of identifiable PHI by "covered entities"—health care providers that transmit health information electronically, health plans, and health care clearinghouses. However, several exceptions to the general rule exist. Where an exception applies, the relevant entities may exchange identifiable electronic health information without first obtaining the individual's written permission.

Most salient, no authorization is required to share PHI (except for psychotherapy notes) for the purpose of "treatment, payment, or health care operations," provided appropriate security processes to transmit the data are in place and provided each custodian of the PHI in the process applies appropriate security safeguards. Covered entities may contract with other organizations for these purposes, making the organizations "business associates" under HIPAA. Business associates carry the same legal liability for breaches as the covered entities they serve, and they

may not use HIPAA-protected identifiable health information for their own business purposes.

The HITECH Act brought third-party HIE efforts definitively into the HIPAA fold.[39] Organizations that provide PHI data transmission or EHR services to a covered entity are automatically deemed business associates under HIPAA. Further, under HITECH, business associates are not merely accountable by contract, they are directly accountable to HHS for compliance with applicable portions of HIPAA's Privacy and Security Rules. Both HHS and state attorneys general have authority to enforce HIPAA through civil and criminal proceedings. In summary, HITECH preserved the existing Privacy Rule exception permitting HIE for treatment, payment, or health care operations purposes, but strengthened the accountability of nonprovider organizations involved in such exchanges.

Health care providers, however, have long behaved as though HIPAA's Privacy Rule constrains their ability to participate in HIE—and it is not clear whether they misunderstand the rule or instead deploy a misconception as a pretext for decisions not to participate in HIE for other reasons.[40] Work by the Health Information Security and Privacy Collaboration (HISPC), convened by ONC and the Agency for Healthcare Research and Quality (AHRQ) in 2005, identified considerable misunderstanding among stakeholders about HIPAA's authorization requirements.[10,11] Things had not significantly improved when ONC took another look at the issue in 2015, at a time when most hospitals and physicians used EHRs daily.[26]

The nature of the misunderstanding is simple: the Privacy Rule provides that disclosures that fall within the treatment-and-operations exception require no separate patient authorization beyond the general consent for medical treatment, but some providers have nevertheless insisted on seeking one.[10] A patchwork of organizational policies for patient consent has resulted. Both opt-out decisions by patients and the variation in policies across providers have served as barriers to the free flow of health information for treatment purposes.

A second misconception is that covered entities that disclose PHI could be liable under HIPAA for the acts of downstream data recipients. A lawyer's worst-case scenario is that a hospital client scrupulously adheres to HIPAA's rules regarding the transfer of PHI to other covered entities and their business associates, but one of those recipients subsequently acts irresponsibly and breaches the confidentiality of the

information, triggering litigation and enforcement actions. Why, the lawyer may counsel, take the risk of sharing information?

Both these notions—that HIPAA requires written authorization for HIE and that liability flows upstream to the discloser who did everything right—are incorrect. Yet the perceptions have constrained progress toward HIE. For instance, concerns about liability for downstream breaches were reportedly one of the chief factors obstructing the growth of an early community HIE effort in Santa Barbara, California.[9] Although liability concerns can in theory be addressed in the contracts executed among the parties engaged in HIE, that case study illustrates that reaching agreement can be arduous. The more contentious the negotiations, the easier it is for providers to simply decline to participate in HIE. Additionally, providers who share health information may be concerned about reputational harm from publicity about breaches by downstream users, even if they do not have legal liability.

The persistence of misguided concerns about HIPAA requirements is striking in light of the dearth of private litigation and federal enforcement actions that would signal that a real liability threat exists. What explains the tenacity of unduly conservative HIPAA interpretations? Risk-averse legal counsel can have a surprising amount of influence within organizations. In-house lawyers often see their primary role as minimizing the organization's liability, as opposed to helping the organization achieve its mission, and institutional leaders may judge counsel's performance primarily based on the metric of liability. In large provider organizations, general counsel may delegate HIPAA compliance responsibilities to lower-level personnel who are overly compliance-focused and whose interpretations of HIPAA may go unchallenged. Outside counsel and consultants, too, may overemphasize liability risks because this reinforces the importance of the services they provide to the organization. Whatever the reason, misconceptions have been hard to dislodge.

Recent Developments

Recently issued guidance documents leave no room for doubt about downstream liability for HIE under HIPAA. In January 2016, ONC and the HHS Office for Civil Rights (OCR), the agency that enforces HIPAA, jointly issued 2 fact sheets in order to clarify how providers may exchange PHI under HIPAA for treatment and operations purposes.[41-43] The fact sheet on permitted disclosures for treatment purposes states in

simple language that a provider who discloses PHI to another provider in a permitted, secure manner is not liable for breaches by the recipient. To the contrary, "the receiving physician, as a CE [covered entity] itself, is responsible for safeguarding the PHI and otherwise complying with HIPAA." Similarly, when sending PHI to business associates, the sending providers "are not responsible for what the BA does with the PHI once it has been disclosed permissibly and securely." The second fact sheet states the same regarding disclosures for operational purposes such as quality-of-care assessments. Both sheets include examples of permissible information sharing through HIE.

Efforts to further educate the legal and provider communities are ongoing. Section 4004 of the Cures Act, for example, directs ONC to continue to issue "guidance on common legal, governance and security barriers" to HIE.[1] Section 4006(a)(2) directs the HHS secretary (in conjunction with OCR) to further educate providers about their ability to engage in HIE to care for their patients and improve health.

Given these developments, it would be difficult for any informed lawyer to maintain the argument that HIPAA is a reason not to engage in HIE. Though confusion may persist within some provider organizations about what the overall framework of state and federal privacy laws requires, HIPAA's rules are now explicated quite clearly. Thus, as ONC implied in a recent report to Congress,[44] HIPAA privacy concerns may be being used as a rationale to not exchange data when it is not in an organization's business interest to do so.

There is one aspect of HIPAA, however, that does create a barrier to HIE: as discussed earlier, it allows states to maintain privacy laws that are stricter than HIPAA. Congress could have designed HIPAA so as to preempt, or trump, stricter state laws, but chose not to. The result has been to preserve what is widely agreed to be the most substantial legal barrier to the growth of HIE[26]: varying state requirements for patient consent.

Inconsistent State-Law Requirements for Patient Consent

A complex web of state laws protects the confidentiality of medical records.[45] A given state often has multiple laws pertaining to different types of health information, and laws vary from state to state. Many state laws preceded HIPAA, dating to the 1970s and 1980s, when

concerns about discrimination on the basis of health conditions were at a fever pitch. The state landscape is particularly varied because, as is discussed later, some states have modernized their laws to explicitly address electronic health information sharing while others have not.[30]

About half of states have laws applying to hospitals and/or health care professionals,[46] but there are also many specialized laws that cover specific data holders (for instance, schools, day care facilities, or correctional facilities) or data types. There are also state laws specifying when minors may control their medical records, although variations in these laws are beyond the scope of our HIE-focused review.

State-law requirements for consent are often more stringent than HIPAA, and they fall into two buckets. The first bucket considers permission for electronic exchange as an activity.[47] For example, Minnesota requires written consent to release any and all health information outside of an emergency.[48] The second bucket is state laws requiring special permission to exchange specific types of health information. In addition to general health privacy statutes, some states have laws relating to particular types of sensitive data, such as information about substance abuse, mental health, HIV/AIDS, other sexually transmitted infections, genetic testing, and disability.[7,48,49] A recent analysis found, for example, that about a third of states have mental health privacy laws with consent provisions that are more restrictive than HIPAA.[50] Adding to the complexity, an additional layer of federal laws, discussed later, imposes consent requirements for some of these same classes of sensitive information (Table 3). Thus, the web of laws governing patient consent is multidimensional: both federal and state, and relating to both what types of information may be shared and who may share with whom.

The thicket of state and federal laws makes it arduous to identify all applicable laws and the segments of a patient's record to which they apply, increasing the cost of engaging in HIE, creating bewilderment about what is allowed, and fueling reluctance to share health information both within and across states. Two substantial research initiatives, one in 2006-2009[51] and another in 2016,[48] identified "significant confusion" among stakeholders about when consent is required under state law. The Health Information Security and Privacy Collaboration (HIPSC) project, initiated by ONC and AHRQ in 2006, concluded that "it is virtually impossible for health care stakeholders to track and maintain knowledge of all these legal factors. . . . As a result, health care stakeholders delay or fail to exchange information due to liability concerns."[51] Nearly a

Table 3. Federal and State Laws Applicable to Selected Types of Health Information

Type of Information	Subject to Federal "Part 2" Regulations?	Subject to Federal Regulations on Veterans' Records?	Subject to Varying State Requirements for Patient Consent?
Substance abuse disorders/treatment	Yes	Yes	Yes
Mental health disorders/ treatment (other than substance abuse)	No	Yes	Yes
Other information	No	No	Yes

decade later, a study by the National Governors Association documented the persistence of the problem, indicating that despite tenacious efforts, not enough progress has been made to create common understandings or uniform laws. Providers operating in multiple states tend to adopt policies adhering to the requirements of the most stringent state, the report concluded, which "results in a situation where optimal information flow does not occur."[48]

Thus, variation in state-law consent requirements inhibits HIE. A rare study quantifying the effect of this legal barrier on engagement with electronic data systems found that state privacy laws restricting hospitals' ability to disclose health records reduced hospitals' adoption of EHRs by 24% over the 1997-2005 period.[8]

Recent Developments

A great deal of thoughtful work by state officials and scholarly commentators has gone into mapping the problem of state-law variation and recommending solutions. These efforts have provided clear road maps forward, but have yet to inspire much action. The HISPC project, involving experts from 34 states, used focus group research to identify laws and business practices that were obstructing HIE. The collaborative

then examined a variety of alternative solutions and developed tools and resources for states interested in addressing these barriers.[32] The 2009 HISPC report on consent issues revealed much about the complexity of the issues but provided few substantive decisions about the optimal approach to patient consent.[51] No consensus was reached, for instance, on whether patient consent should be required by states at all; or, if it is, about whether patients should be asked to opt in or opt out of information sharing. To resolve interstate conflicts of law, the collaborative recommended that states develop interstate compacts, in which 2 or more states execute a voluntary, legally binding agreement about which rules will govern.

By 2016, when the National Governors Association took another look at this issue, no interstate compacts had emerged. Interviews with more than 90 state officials and other stakeholders found that there was consensus that states needed harmonized laws, but no appetite for undertaking the difficult political work involved.[48]

Although harmonization remains elusive, some states have taken steps individually to modulate their privacy laws' stringency in order to facilitate HIE. For example, Hawaii, Kansas, Wisconsin, and Utah have passed legislation to allow HIE in accordance with HIPAA, eliminating more restrictive state requirements.[48] Nevada, Ohio, and Colorado adopted similar laws for exchanges of electronic health information only.[48] Arizona shifted to an opt-out consent regime for HIE.[52] New York recently proposed new consent rules to make data more available for exchange.[53] Maryland modified the privacy laws applicable to its insurers so that they could exchange identifiable claims data with physician practices.[54] These steps have been helpful. However, a recent review of state laws relating to HIE concluded that much work remains to be done. As of 2016, among 31 states with laws addressing privacy and HIE, 16 followed the opt-out approach, 8 described an opt-in process, and the rest adopted other approaches to HIE participation. Twenty-three states imposed specific confidentiality requirements on HIE users and 5 mentioned confidentiality without providing specific requirements.[45]

As an alternative to legal harmonization, technical solutions for ensuring compliance with varied state laws have also been pursued. From 2013 through 2015 ONC nurtured the development of a technical standard called Data Segmentation for Privacy, or DS4P. DS4P is a standard for adding a metadata tag to an electronic document to flag it as needing patient consent before being disclosed. Historically, it has been difficult

or impossible for providers to separate out parts of a patient's record that are subject to special consent requirements from parts that are not. The DS4P tag can help address this problem, although there is some disagreement within the health IT community about whether DS4P is ready to be implemented at scale.

In October 2015, ONC published DS4P as an optional feature that EHR vendors could include in their new products effective January 1, 2017, and which ONC would test and certify. The standard has since been endorsed by the Substance Abuse and Mental Health Services Administration (SAMHSA), which administers federal privacy regulations relating to records of federally funded substance abuse treatment. If health care providers purchase EHRs with DS4P capability, they can reduce the risk of inappropriately disclosing private information and the challenges of navigating different state-law requirements. However, as long as DS4P remains an optional feature of certified EHR technology, providers will have to request—and pay extra for—the capability. And, as with any technical standard that depends on coding and implementation specifications, DS4P's power could be undermined by nonstandard implementation.

Even with data segmentation, state-law variations in consent requirements may continue to chill the growth of HIE because of their effects on patient participation in information sharing. Patient participation rates in HIE in an opt-out versus an opt-in regime are substantially different, likely reflecting humans' well-documented tendency to select the default option when their choice is structured to include one.[55,56] States that adopted opt-out consent regimes in the wake of HITECH have reported opt-out rates from HIE in the 2%-5% range.[57-59] Other research shows that when state law required patients to opt in to use of their health data for research purposes, only 19% of patients did so.[60] The lower participation rate could be attributable to the different use to which the data would be put, but the necessity of shifting off the default choice likely played a role as well.

When patient participation in HIE is low, providers' interest in information exchange suffers too. Providers conclude, with reason, that the value of participating in HIE is lower if the data are less complete.[35] An expert panel convened by ONC concluded that opt-out and opt-in consent are equally viable in terms of respecting autonomy and protecting privacy[61]—but they clearly have dramatically different consequences for the robustness of HIE.

In summary, limited progress has been made in addressing state-law provisions that impede HIE. Inconsistency remains a barrier. Even within a state, providers may have to navigate multiple laws relating to different parts of a patient's medical record. Data segmentation capabilities could provide considerable relief, but only to those who adopt DS4P-enabled EHR systems and are confident about the types of data that need to be specially tagged.

Special Federal Protections for Particularly Sensitive Health Information

A number of federal-law provisions impose heightened patient consent requirements for disclosure of certain kinds of sensitive health information, similar to the ways state health privacy laws do. Like the state laws, these laws have been identified as barriers to HIE because they make different aspects of a patient's health record subject to different requirements.

The most important federal laws relate to veterans, genetic information, and alcohol and substance abuse treatment. For veterans, 38 U.S.C. § 7332 provides heightened confidentiality protections for information relating to drug and alcohol abuse, HIV infection, and sickle-cell anemia. Specific written consent for disclosure of this information is required unless narrow statutory exceptions apply. The most helpful exception permits information exchange among health care providers within the Department of Veterans Affairs—but does not extend to providers outside that department even when the exchange is for treatment purposes.

The Genetic Information Nondiscrimination Act of 2008 (GINA)[62] has been counted among the federal-law barriers to HIE.[7] GINA precludes employers from disclosing genetic information they hold about employees except by written request of the employee, unless narrow exceptions apply. It also amends HIPAA to specify that genetic information is protected health information for purposes of HIPAA's Privacy Rule and prohibits health plans that are HIPAA-covered entities from using or disclosing genetic information for underwriting purposes.[39] These provisions in theory could affect HIE where health information is generated by a provider in the employer organization or in an integrated health system that is both a health plan and a provider.

Citing these provisions as a barrier to HIE is a mistake, however. The health plan provision does not affect disclosures made for nonunderwriting purposes, including treatment. Further, GINA's employer provision does not affect disclosures that are otherwise permitted under HIPAA. Continued expressions of concern about GINA as a constraint on HIE, however, are evidence of how poor the understanding is at an operational level of which rules apply to which data.

A final source of confusion constraining HIE is the federal 42 C.F.R. Part 2 rules, which are enforced by SAMHSA. These rules restrict the conditions under which identifiable health information held by a federally funded program that provides substance use disorder services can be disclosed.

The Part 2 regulations were promulgated in 1975 at the direction of Congress[63] out of concern that confidentiality and discrimination worries might be keeping patients from seeking substance abuse treatment. The authorizing legislation and subsequent regulations apply to disclosure of any information obtained by a federally assisted drug or alcohol abuse program that would identify a patient as an alcohol or drug abuser. Covered programs include those that receive federal grants or Medicare or Medicaid payments, including specialized programs and staff within general medical facilities, as well as any federally funded health insurance used to obtain substance use disorder benefits.[64] Part 2 requires that specific patient consent be given (or a court order produced) to disclose records and prohibits onward sharing by the recipient. Unlike HIPAA, there is no treatment exception, although disclosures can be made without consent to "qualified service organizations" providing ancillary services like laboratory tests.

Recent Developments

In March 2017, SAMHSA finalized a revised rule that liberalizes the Part 2 consent rules.[65] It permits patients to designate a general entity, such as an HIO and its affiliated providers, to receive their health information. In contrast, the original Part 2 rules stipulated that when patients released their information, they had to name each individual and organization that could receive the data. This meant that patients could not give general permission for an HIO to share information across its current and future members.

The rule change was intended to facilitate HIE for treatment purposes and to better integrate substance abuse patients into integrated health care models. It greatly improves the ability of HIOs to make information flow across evolving networks of member providers, and it allows an individual to authorize an HIO to store the information (as opposed to sending to a specific provider). However, it retains the requirement of a separate patient consent for release of drug and alcohol information; a general consent for HIE that applies to all types of information is insufficient. Additionally, it does not permit the HIO or its member providers to pass the information along to other providers who are treating the patient but are not members, unless separate consent is obtained. Therefore, the substance abuse regulations will continue to serve as an obstacle—albeit a smaller one—going forward. Further, it may be some time before organizations modify their policies and procedures to take advantage of the revised Part 2 rules.

Additional action relating to Part 2 may be on the horizon. The 21st Century Cures Act, section 11002, directs the HHS secretary to convene stakeholders within a year to determine the effect of the Part 2 regulations on patient care, health outcomes, and privacy.[1] This certainly could include review of the effect of the consent requirement for substance abuse on HIEs and impacts on patient care. It could also address reports that providers are often confused about whether they are a covered organization under Part 2. For example, many providers of mental health care (but not substance abuse disorder treatment) reportedly misperceive themselves as subject to Part 2 obligations even though they do not hold themselves out as being substance abuse providers.[48] Although these steps within the Cures Act may be helpful, the act does not ease the privacy protections in the original statute pursuant to which Part 2 was promulgated.[63]

In July 2017, the President's Commission on Combating Drug Addiction and the Opioid Crisis moved the ball further by recommending in its draft report that the Part 2 regulations be aligned with HIPAA's privacy rules.[66] Citing the written consent requirements for substance abuse records as a barrier to effective care for opioid-addicted patients, the commission essentially called for a treatment exception to the consent mandate. Legislation that would do the same was introduced in the House in July.[67]

Repealing the special consent requirements and allowing antidiscrimination laws to do the work of protecting patients against discrimination

based on their substance abuse treatment are the surest ways to overcome this roadblock to HIE. Unless and until this occurs, the most promising way forward is technical. As discussed earlier, the DS4P standard will help address some of the difficulties in cordoning off substance abuse treatment data within the EHR. The rest of the patient's record, at least, can then be exchanged.

Failed Efforts to Establish a Unique Patient Identifier

A final legal barrier to HIE is the repeated failure of efforts to establish a unique patient identifier number (UPI) that is universal to all health records. A highly reliable method of matching records to patients is needed to ensure that a patient's EHR contains full, accurate information, but this has not been part of the national strategy for accelerating HIE.[4] Omissions and errors in matching can lead to serious patient harm and mistakes in disclosing sensitive information to the wrong persons.[10] One way to match patient records is for organizations to use algorithms to try to match patients on the basis of identifying characteristics such as gender, date of birth, Social Security number, and address. To date, algorithmic matching has offered a viable alternative to a UPI, but no algorithm is perfect.

Given the vast number of matches made daily, even a tiny error rate can affect large numbers of patients. But error rates can be substantial: a survey of 128 health care leaders found that nearly half experienced "false-negative" matching errors of 8% or higher (some as high as 20%); 40% experienced "false-positive" errors at this level; and 19% attributed one or more adverse events in the past year to a matching error.[68] Concerns about mismatches may account for the survey finding that 8 in 10 community HIEs view difficulties achieving accurate patient record matching as a barrier to progress on HIE.[36]

Recognizing that a UPI is the natural solution, HIPAA instructed HHS to issue a UPI standard. However, UPI proposals encountered vocal political resistance from privacy advocates, prodding Congress to intervene in 1999 to prevent HHS from promulgating any such standard, or even expending money to assist in its development, without congressional approval.[69] Objections reflected concerns that without adequate privacy and security protections in place, privacy risks are

amplified when information flows freely across boundaries, with the UPI as the technological conduit. Arguably, such complaints overlook the privacy and security risks posed by the widespread use today of alternative identifiers, such as birthdates and Social Security numbers.[69] The privacy objections, at their core, are protests of the very concept of HIE: the UPI is a means of accelerating a future that causes privacy advocates great disquiet.

The legal impediment erected by Congress to UPI implementation has hampered the growth of HIEs, particularly beyond the local and regional levels.[12,69] Not only does the lack of UPI pose a technical barrier to linking records, but by elevating the risk of inaccurate matches and missed records, it heightens the risk of erroneous patient care decisions. Recognition that record matching is imperfect feeds providers' fears that malpractice liability may ensue from acting on false or incomplete information. Providers may also worry that erroneous matches will lead them to inadvertently share information about a patient who has directed that her information not be disclosed. These concerns reinforce providers' reluctance to exchange records electronically.[2,69]

Recent Developments

There are signals in the Cures Act that a solution to the UPI problem may be on the way. Section 4007 directs the General Accountability Office to conduct a study within 2 years on ONC policies and activities and the practices of other stakeholders "to ensure appropriate patient matching to protect patient privacy and security." The study's explicit objectives are "improving matching rates" and "reducing matching errors." The study must determine whether ONC could improve patient matching by "defining additional data elements" or other means.

Section 4003 of the Cures Act also calls for a Health Information Technology Advisory Committee to recommend standards and specifications to promote interoperability, which are likely to include matching methods. The committee is instructed to target its efforts to identifying "technology that provides accurate patient information for the correct patient, including exchanging such information, and avoids the duplication of patient records."

If these studies point toward a UPI as the preferred matching method, it may embolden HHS to seek congressional approval for a new standard. In the interim, ONC, in partnership with medical malpractice experts,

could ease providers' concerns by continuing to educate them about their liability for malpractice. It is unlikely that under a negligence standard they would be held liable for care decisions based on information they could not reasonably have known was missing or inaccurate. Calming this outsized anxiety could encourage broader provider participation in HIE.

Information Blocking

Information blocking occurs "when persons or entities knowingly and unreasonably interfere with the exchange or use of electronic health information."[44] Examples of blocking by a provider include the following: refusing to transmit patient information to a competing organization electronically and insisting on fax transmission; ignoring a patient's instruction to send his health information to a third party; refusing to share data with others due to purported concerns about security at the recipient organization; and deploying products with limited interoperability or data export capabilities.[44,70] Blocking by vendors occurs when, for instance, a vendor prices its products so high that providers cannot afford to buy interoperable systems;[48] charges a fee every time a patient's information is sent, received, or searched out; refuses to exchange information with certain organizations or systems; or requires providers to use direct, secure connections for information transfer that are prohibitively expensive.[44]

Information blocking is not, strictly speaking, a legal barrier to HIE—rather, it is a market barrier that until recently the law had not intervened to correct. It arises because of competitive disincentives to participate in HIE. It can be to providers' economic advantage to make patient information hard for others to access, because it makes it more difficult for patients to switch to other providers and for physicians to refer patients out of network. Vendors also maximize their competitive position by holding patient data within walls that providers must pay to pass through.[71] Exchanging data only within these walled gardens makes it easier for vendors to attract and retain customers. Provider and vendor disincentives may reinforce each other: it is easier for a provider to decline to engage in HIE when vendor HIE costs are high, and providers may not demand low-cost HIE options from vendors.

Although the prevalence of information-blocking practices has not been systematically measured, exploratory research and the volume of unsolicited complaints about information-blocking practices suggest it is a significant problem.[44] A recent survey of 60 individuals leading HIE efforts found that 50% reported that EHR vendors routinely engaged in blocking and another 33% said it occurred occasionally. Further, 25% said that hospitals and health systems routinely engaged in blocking and 34% said they did so occasionally. Among the forms of blocking reported, one notable finding was that 50% of respondents said that hospitals and health systems routinely or sometimes "use HIPAA as a barrier to patient health information sharing when it is not."[70]

Recent Developments

Following a crescendo of complaints about information blocking, in 2014 Congress directed ONC to investigate the practice. ONC's February 2015 report concluded that "while the evidence is in some respects limited, there is little doubt that information blocking is occurring and that it is interfering with the exchange of electronic health information."[44] The report outlined the need for additional legal tools to prevent information blocking and recommended specific actions for Congress to take.

In 2016, Congress responded by prohibiting certain types of information blocking as part of the 21st Century Cures Act. Section 4002 of the act requires the HHS secretary to issue regulations specifying that refraining from information blocking is a condition of certification of vendors' EHR products. Section 4004 provides a basic definition of information blocking, subject to elaboration in forthcoming regulations. The broad definition encompasses practices that are "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information" and that the IT developer, exchange, or network knows or should know is likely to have that effect. (The definition for providers is more lenient, applying only where the provider "knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.") Section 4004 empowers the federal Office of the Inspector General to investigate claims of information blocking and impose stiff financial penalties on IT developers, exchanges, and network organizations. In contrast, providers who engage in the practice

are merely "referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law," to be described in rulemaking by the HHS secretary.

The Cures Act's focus on IT organizations (as opposed to providers) is notable. This focus is understandable in light of the fact that these entities built their business on financial incentives for health IT adoption that were financed by taxpayers. However, a portion of the responsibility for impeding HIE rests with provider organizations and their lawyers, whose persistent belief in privacy myths contributes to information blocking.

In addition to prompting action in the Cures Act, ONC's report has impacted state legislators' thinking. In 2015, Connecticut passed a law making information blocking illegal under the state's unfair trade practices law, stipulating that patients (not providers) are the owners of their own medical records, and providing substantial information rights to patients.[72]

It remains to be seen how the Cures Act's information-blocking provisions will play out, and in particular, what actions will be taken against providers. Nevertheless, the recent developments on information blocking are very promising and could substantially address the problem.

Discussion

To summarize, although some legal barriers to HIE persist, many have been ameliorated—in some cases, simply by clarifying what the law actually requires. HIPAA presents no obstacles whatsoever to sharing PHI for treatment and operations purposes and imposes no liability for downstream privacy breaches on disclosing entities that follow the rules. There can be no real disagreement on these points given the government's recently issued fact sheets.[41,42] Development of a UPI has not yet occurred, but action on the problem of inaccurate patient record matching will be taken under the Cures Act.[1] The Cures Act also put the legal architecture in place to begin to combat information blocking.[1] Its provisions relating to blocking by vendors are robust, and enforcement is likely to be a high priority given the attention the issue has garnered.[73] It is less clear whether the government will take strong action in response to information blocking by health care providers, where the act gives

HHS greater discretion. However, providers tend to be highly averse to even modest legal risks, which may have deterrent value.

Patient consent requirements under state and federal law are the most important remaining legal barrier to HIE expansion,[45,47,48] but here too, some progress has been made. The recent liberalization of the Part 2 rules pertaining to substance abuse data will facilitate broader information exchange, although a one-time patient consent is still required. The DS4P standard will allow segmentation of sensitive data so that even if specific consent is not obtained to disclose certain types of sensitive information, at least the bulk of the patient's record can be shared. Still, the complexity and inconsistency of state laws will remain off-putting to many providers.

Although no legal provisions prevent HIE, there is still much to be done to make it easy to routinely share information electronically. Ongoing work to simplify the legal regime should include developing the UPI,[36] making further efforts to disabuse providers of their legal misunderstandings, promoting and requiring the DS4P standard to accelerate widespread adoption, and reconsidering periodically whether the time is right for states to loosen consent requirements.

Efforts to simplify the legal regime would benefit any HIE effort, but may be particularly critical for HIOs. As small organizations with limited resources, HIOs are disproportionately impacted by regulatory complexity[74] alongside the changes to their technical infrastructure and governance that must occur when regulations change. In addition, given that a population's health needs are best served when all its members' health information is available for treatment purposes, if legal concerns prevent the participation of even a single provider organization, the impact on the value of the whole network can be substantial. A similar impact can occur across a national HIE network if a single but significant provider organization chooses not to participate.

However, perhaps more important than addressing the remaining legal complexities is building a strong business case for HIE participation. At this point, legal concerns may be serving as a proxy for reservations about joining HIEs that are primarily financially motivated and unrelated to potential liability costs. For many providers and vendors, the perceived costs and risks (including risk of competitive harm) continue to outweigh the perceived benefit.[4,75]

Although a full discussion of the cost-benefit equation around HIEs is beyond the scope of this article, the essence is that there is typically

significant up-front cost to join HIOs or to engage in HIE, as well as ongoing maintenance costs.[2] In addition to direct participation costs, costs arise in the form of provider time to redesign workflows to integrate HIE into frontline care. Further, when HIE solutions are not well integrated, it can take extra time to use them, hampering provider productivity.[2,76,77] When providers are paid on a fee-for-service basis, an additional cost comes in the form of lost revenue from reducing redundant services (for example, tests that the provider sees the patient has already undergone). Finally, HIE makes it easier for patients to seamlessly switch health care providers or obtain some services out of network, potentially resulting in lost volume and revenue.[35]

In contrast to these real and potential costs, the benefits are less tangible. Professional obligations and reputational benefits may drive some providers to engage in HIE.[78] There are also federal (and some state) incentives for joining HIEs. In particular, meaningful use measures that require summary care record exchange during care transitions, ePrescribing, and HIE with public health stakeholders have created incentives. More incentives may come, depending on how CMS implements the Medicare & CHIP Reauthorization Act of 2015. However, the thresholds for satisfying the criteria for receiving incentives have been low, and in some cases providers can opt out of needing to meet them. Strengthening HIE is important to the success of delivery and payment reform efforts that seek to achieve high-value care. HIE is essential to ensure that, at both individual and population levels, providers and administrators have the information they need to make safe, effective, and efficient care decisions.

The policy options to increase HIE participation by providers are straightforward: increase the benefits, decrease the costs, or require participation. CMS has indicated its strategy may involve all three, with a focus on financial rewards and further clarifications of federal privacy law in the near term and the imposition of quality standards that include HIE over the longer term.[25] Potentially, financial rewards for HIE could take either direct or indirect forms—that is, providers could be paid for engaging in HIE or for improved efficiency and outcomes that are practically achievable only with HIE. The focus on incentives seems appropriate in light of empirical evidence that incentives reduce the chilling effect of privacy laws on HIE participation,[35] although the HITECH Act's $30 billion price tag seems a substantial investment already. When CMS and ONC requested comments from stakeholders

on actions that would accelerate HIE, commentators focused heavily on incentives. For example, one recommendation was to add specific reimbursement codes for HIE implementation and use.[25]

Finally, CMS and HHS continue to deepen their commitment to value-based and bundled payments, which by their very nature reward well-integrated care. As a greater share of physician and hospital compensation comes to depend on using comprehensive digital health information in an effective way, the business case for HIE will strengthen. As it does, the perceived legal barriers to HIE may further fade.

References

1. 21st Century Cures Act, Pub L No. 114–255 (2016).
2. Fontaine P, Ross SE, Zink T, Schilling LM. Systematic review of health information exchange in primary care practices. *J Am Board Fam Med*. 2010;23(5):655-670. https://doi.org/10.3122/jabfm.2010.05.090192.
3. Holmgren AJ, Adler-Milstein J. Health information exchange in US hospitals: the current landscape and a path to improved information sharing. *J Hosp Med*. 2017;12(3):193-198.
4. Halamka JD, Tripathi M. The HITECH era in retrospect. *N Engl J Med*. 2017;377(10):907-909.
5. Unertl KM, Johnson KB, Lorenzi NM. Health information exchange technology on the front lines of healthcare: workflow factors and patterns of use. *J Am Med Inform Assoc*. 2012;19(3):392-400.
6. Christiansen J. Legal speed bumps on the road to health information exchange. *J Health Life Sci Law*. 2008;1:1-49.
7. Weiser SJ. Breaking down the federal and state barriers preventing the implementation of accurate, reliable and cost effective electronic health records. *Ann Health Law*. 2010;19:205-211.
8. Miller AR, Tucker CE. Privacy protection and technology diffusion: the case of electronic medical records. *Manage Sci*. 2009;55(7):1077-1093. https://doi.org/10.1287/mnsc.1090.1014.
9. Miller RH, Miller BS. The Santa Barbara County care data exchange: what happened? *Health Aff (Millwood)*. 2007;26(5):w568-w580. https://doi.org/10.1377/hlthaff.26.5.w568.
10. Dimitropoulos L, Rizk S. A state-based approach to privacy and security for interoperable health information exchange. *Health Aff (Millwood)*. 2009;28(2):428-434. https://doi.org/10.1377/hlthaff.28.2.428.

11. Dimitropoulos LL, RTI International. *Privacy and Security Solutions for Interoperable Health Information Exchange: Nationwide Summary*. Chicago, IL: Agency for Healthcare Research and Quality, Department of Health and Human Services; 2007. http://bok.ahima.org/PdfView?oid=73028. Accessed August 3, 2017.
12. Greenberg MD, Ridgely MS, Hillestad RJ. Crossed wires: how yesterday's privacy rules might undercut tomorrow's nationwide health information network. *Health Aff (Millwood)*. 2009;28(2):450-452. https://doi.org/10.1377/hlthaff.28.2.450.
13. Everson J. The implications and impact of 3 approaches to health information exchange: community, enterprise, and vendor-mediated health information exchange. *Learning Health Sys*. 2017;1(2):e10021. https://doi.org/10.1002/lrh2.10021.
14. Vest JR, Gamm LD. Health information exchange: persistent challenges and new strategies. *J Am Med Inform Assn*. 2010;17(3):288-294. https://doi.org/10.1136/jamia.2010.003673.
15. Adler-Milstein J, Lin SC, Jha AK. The number of health information exchange efforts is declining, leaving the viability of broad clinical data exchange uncertain. *Health Aff (Millwood)*. 2016;35(7):1278-1285. https://doi.org/10.1377/hlthaff.2015.1439.
16. Adler-Milstein J, Bates DW, Jha AK. Operational health information exchanges show substantial growth, but long-term funding remains a concern. *Health Aff (Millwood)*. 2013;32(8):1486-1492. https://doi.org/10.1377/hlthaff.2013.0124.
17. Adler-Milstein J, Bates DW, Jha AK. A survey of health information exchange organizations in the United States: implications for meaningful use. *Ann Intern Med*. 2011;154(10):666-671. https://doi.org/10.7326/0003-4819-154-10-201105170-00006.
18. Adler-Milstein J, Bates DW, Jha AK. US regional health information organizations: progress and challenges. *Health Aff (Millwood)*. 2009;28(2):483-492. https://doi.org/10.1377/hlthaff.28.2.483.
19. Adler-Milstein J, McAfee AP, Bates DW, Jha AK. The state of regional health information organizations: current activities and financing. *Health Aff (Millwood)*. 2008;27(1):w60-w69. https://doi.org/10.1377/hlthaff.27.1.w60.
20. eHealth exchange overview. The Sequoia Project. http://sequoiaproject.org/wp-content/uploads/2016/05/eHealth-Exchange-Overview-Feb-2016-v2.pdf. Published February 2016. Accessed December 13, 2017.
21. What is Carequality? The Sequoia Project website. http://sequoiaproject.org/carequality/what-we-do/. Accessed December 13, 2017.

22. CommonWell Health Alliance. Overview of CommonWell services. http://www.commonwellalliance.org/wp-content/uploads/2014/10/CommonWell-Concepts.Feb_2017.final_.pdf. Published February 2017. Accessed December 13, 2017.
23. CommonWell Health Alliance. Carequality and CommonWell Health Alliance agree on connectivity and collaboration to advance interoperability. http://www.commonwellalliance.org/news/carequality-commonwell-health-alliance-collaboration/. Published December 13, 2016. Accessed December 13, 2017.
24. US Senate Committee on Health, Education, Labor & Pensions. Hearing on implementation of the 21st Century Cures Act: achieving the promise of health information technology. 115th Cong. October 31, 2017. https://www.help.senate.gov/hearings/implementation-of-the-21st-century-cures-act-achieving-the-promise-of-health-information-technology. Accessed December 13, 2017.
25. Office of the National Coordinator for Health Information Technology. *Principles and Strategy for Accelerating Health Information Exchange (HIE)*. Washington, DC: Department of Health and Human Services. https://www.healthit.gov/sites/default/files/acceleratinghieprinciples_strategy.pdf. Published August 7, 2013. Accessed December 13, 2017.
26. Office of the National Coordinator for Health Information Technology. *Connecting Health and Care For the Nation: A Shared Nationwide Interoperability Roadmap*. Washington, DC: Department of Health and Human Services. https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf. Published 2015. Accessed August 2, 2017.
27. Office of the National Coordinator for Health Information Technology. *2016 Report to Congress on Health IT Progress: Examining the HITECH Era and the Future of Health IT*. Washington, DC: Department of Health and Human Services. https://dashboard.healthit.gov/report-to-congress/2016-report-congress-examining-hitech-era-future-health-information-technology.php. Published 2016. Accessed May 16, 2017.
28. Holmgren AJ, Patel V, Charles D, Adler-Milstein J. US hospital engagement in core domains of interoperability. *Am J Manag Care*. 2016;22(12): e395-e402.
29. Office of the National Coordinator for Health Information Technology. Electronic health information exchange performance reported to the Medicare EHR Incentive Program, 2014. Washington, DC: Department of Health and Human Services.

https://dashboard.healthit.gov/quickstats/pages/eligible-provider-electronic-hie-performance.php. Published 2015. Accessed May 16, 2017.

30. Hill JW, Langvardt AW, Massey AP, Reinhart JE. A proposed national health information network architecture and complementary federal preemption of state health information privacy laws. *Am Bus Law J*. 2011;48(3):503-595. https://doi.org/10.1111/j.1744-1714.2011.01120.x.
31. Dullabh P, Parashuram S, Hovey L, Ubri P, Fischer K. *Evaluation of the State Health Information Exchange Cooperative Agreement Program: Final Report*. Chicago: National Opinion Research Center, University of Chicago. https://www.healthit.gov/sites/default/files/reports/finalsummativereportmarch_2016.pdf. Published March 2016. Accessed August 3, 2017.
32. Office of the National Coordinator for Health Information Technology. Health information security & privacy collaboration (HISPC). Washington, DC: Department of Health and Human Services. https://www.healthit.gov/policy-researchers-implementers/health-information-security-privacy-collaboration-hispc. Updated June 5, 2013. Accessed May 16, 2017.
33. Markle Foundation. *Connecting for Health: a Public-Private Collaborative Convened by the Markle Foundation: Statement of Purpose*. New York, NY: Markle Foundation. https://www.markle.org/publications/957-connecting-health-public-private-collaborative-convened-markle-foundation. Published April 3, 2006. Accessed May 16, 2017.
34. Health Information Technology for Economic and Clinical Health Act, Pub L No. 111–5 (2009).
35. Adjerid I, Acquisti A, Telang R, Padman R, Adler-Milstein J. The impact of privacy regulation and technology incentives: the case of health information exchanges. *Manage Sci*. 2016;62(4):1042-1063. https://doi.org/10.1287/mnsc.2015.2194.
36. Mathematica Policy Research and Harvard School of Public Health. *Health Information Technology in the United States, 2015: Transition to a Post-HITECH World*. Princeton, NJ: The Robert Wood Johnson Foundation. http://www.rwjf.org/en/library/research/2015/09/health-information-technology-in-the-united-states-2015.html. Published September 18, 2015. Accessed August 3, 2017.
37. Office for Civil Rights, Department of Health and Human Services. Health Insurance Portability and Accountability Act: Security and Privacy. 45 C.F.R. 164 (2002).
38. Health Insurance Portability and Accountability Act, Pub L No. 104–191, 110 Stat. 1936 (1996).

39. Office for Civil Rights, Department of Health and Human Services. Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. 78 FR 5566–5702 (2013).
40. Downing NL, Adler-Milstein J, Palma JP, et al. Health information exchange policies of 11 diverse health systems and the associated impact on volume of exchange. *J Am Med Inform Assoc*. 2017;24(1):113-122. https://doi.org/10.1093/ocw063.
41. Office of the National Coordinator for Health Information Technology and Office for Civil Rights. Permitted uses and disclosures: exchange for treatment. Washington, DC: Department of Health and Human Services. https://www.healthit.gov/sites/default/files/exchange_treatment.pdf. Published January 2016. Accessed May 8, 2017.
42. Office of the National Coordinator for Health Information Technology and Office for Civil Rights. Permitted uses and disclosures: exchange for health care operations. Washington, DC: Department of Health and Human Services. http://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf. Published January 2016. Accessed May 8, 2017.
43. Washington V, DeSalvo K, Mostashari F, Blumenthal D. The HITECH Era and the path forward. *N Engl J Med*. 2017;377(10):904-906.
44. Office of the National Coordinator for Health Information Technology. *Report to Congress: Report on Health Information Blocking*. Washington, DC: Department of Health and Human Services. https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf. Published April 2015. Accessed August 2, 2017.
45. Schmit CD, Wetter SA, Kash BA. Falling short: how state laws can address health information exchange barriers and enablers. *J Am Med Inform Assoc*. 2017. https://doi.org/10.1093/jamia/ocx122. [Epub ahead of print]
46. Pritts J, Lewis S, Jacobson R, Lucia K, Kayne K. *Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Law Requirements for Patient Permission to Disclose Health Information*. Chicago, IL: RTI International. https://www.healthit.gov/sites/default/files/290-05-0015-state-law-access-report-1.pdf. Published August 2009. Accessed August 3, 2017.
47. Office of the National Coordinator for Health Information Technology. State-by-state HIE consent laws. Washington, DC:

Department of Health and Human Services. https://dashboard.healthit.gov/apps/state-health-it-privacy-consent-law-policy.php. Published July 2017. Accessed July 17, 2017.

48. Johnson KB, Block L, Isasi F. *Getting the Right Information to the Right Health Care Providers at the Right Time: A Road Map for States to Improve Health Information Flow Between Providers*. Washington, DC: National Governors Association Center for Best Practices. https://www.nga.org/files/live/sites/NGA/files/pdf/2016/1612HealthCareRightInformation.pdf. Published 2016. Accessed August 3, 2017.
49. Health Information & the Law Project. Disclosure of mental health records with patient consent: 50 state comparison. Project HITL website. http://www.healthinfolaw.org/comparative-analysis/disclosure-mental-health-records-patient-consent-50-state-comparison. Published 2015. Accessed July 31, 2017.
50. Rothenberg LS, Ganz DA, Wenger NS. Possible legal barriers for PCP access to mental health treatment records. *J Behav Health Serv Res*. 2016;43(2):319-329.
51. Delaney-Greenbaum K, Giorgi S, Holm B, et al. *Health Information Security and Privacy Collaboration: Intrastate and Interstate Consent Policy Options Collaborative—Final Report*. Intrastate and Interstate Consent Policy Options Collaborative; 2009.
52. Ariz. Rev. Stat. 36–3801 (2013).
53. Raths D. In New York, statewide HIE re-examining consent model. Healthcare Informatics website. https://www.healthcare-informatics.com/article/hie/new-york-statewide-hie-re-examining-consent-model. Published April 17, 2017. Accessed June 7, 2017.
54. Md. Ins. Code 15–1903, Stat. 15–1903 (2013).
55. Johnson EJ, Bellman S, Lohse GL. Defaults, framing and privacy: why opting in-opting out. *Marketing Letters*. 2002;13(1):5-15. https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf. Accessed August 3, 2017.
56. Thaler RH, Sunstein CR. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New York: Penguin Books; 2008.
57. Lewis MT, Naugle A, Schneider A. *Health Information Exchange Statewide Environmental Scan Findings*. Seattle: Milliman; 2015.
58. Cauthon P. Far fewer than projected patients opting out of health information exchange. Kansas Health Institute News Service. http://www.khi.org/news/article/far-fewer-patients-opt-ing-out-exchange-officials. Published June 14, 2012. Accessed July 12, 2017.

59. Hoyt RE. *Health Informatics: Practical Guide for Healthcare and Information Technology Professionals*. 6th ed. Pensacola, FL: Informatics Education; 2014.
60. McCarthy DB, Shatin D, Drinkard CR, Kleinman JH, Gardner JS. Medical records and privacy: empirical effects of legislation. *Health Serv Res*. 1999;34(1 Pt 2):417-425. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1089011/. Accessed August 3, 2017.
61. Health Information Technology Policy Committee. Letter to David Blumenthal, MD, MPP from Paul Tang, Vice Chair, Health IT Policy Committee (Tiger Team). September 1, 2010. https://www.healthit.gov/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf. Accessed December 13, 2017.
62. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110–233, 122 Stat. 881 (2008).
63. 42 U.S.C. §290dd-2(g) (1974).
64. Wattenberg SA. Frequently asked questions: applying the substance abuse confidentiality regulations to health information exchange (HIE). Washington, DC: Substance Abuse and Mental Health Services Administration, Department of Health and Human Services. https://www.samhsa.gov/sites/default/files/faqs-applying-confidentiality-regulations-to-hie.pdf. Published 2010. Accessed December 13, 2017.
65. Substance Abuse and Mental Health Services Administration, Department of Health and Human Services. Final rule: confidentiality of substance use disorder patient records. 82 Fed. Reg. 6052 (2017).
66. President's Commission on Combating Drug Addiction and the Opioid Crisis. *Interim Report*. Washington, DC: The White House; July 31, 2017.
67. Overdose Prevention and Patient Safety Act. H.R. 3545. 115th Cong., 1st Sess. July 28, 2017.
68. Bipartisan Policy Center. Challenges and strategies for accurately matching patients to their health data. Washington, DC: Bipartisan Policy Center. http://www.redwoodmednet.org/projects/events/20120719/Accurately-Matching-Patients-to-Their-Health-Data.pdf. Published June 2012. Accessed December 13, 2017.
69. Greenberg MD, Ridgely MS. Patient identifiers and the National Health Information Network: debunking a false front in the privacy wars. *J Health & Biomed Law*. 2008;4(1):31-68.
70. Adler-Milstein J, Pfeifer E. Information blocking: is it occurring and what policy strategies can address it? *Milbank Q*. 2017;95(1):117-135. https://doi.org/10.1111/1468-0009.12247.

71. Kendrick DC. Testimony of David C. Kendrick, MD, MPH, Hearing on Achieving the Promise of Health Information Technology: Information Blocking and Potential Solutions. U.S. Senate Committee on Health, Education, Labor and Pensions. July 23, 2015. https://www.help.senate.gov/imo/media/doc/Kendrick.pdf. Accessed December 13, 2017.
72. An Act Concerning Hospitals, Insurers, and Health Care Consumers. Ct. Pub. Act No. 15–146 (2015).
73. White PJ. Statement of P. Jon White, MD before the U.S. Senate Committee on Health, Education, Labor and Pensions. October 31, 2017. https://www.help.senate.gov/imo/media/doc/White5.pdf. Accessed December 13, 2017.
74. Adler-Milstein J, Lin SC, Jha AK. The number of health information exchange efforts is declining, leaving the viability of broad clinical data exchange uncertain. *Health Aff (Millwood)*. 2016;35(7):1278-1285. https://doi.org/10.1377/hlthaff.2015.1439.
75. Adler-Milstein J. Moving past the EHR interoperability blame game. *NEJM Catalyst*, July 18, 2017. https://catalyst.nejm.org/ehr-interoperability-blame-game/. Accessed December 13, 2017.
76. Doebbeling BN, Chou AF, Tierney WM. Priorities and strategies for the implementation of integrated informatics and communications technology to improve evidence-based practice. *J Gen Intern Med*. 2006;21(Suppl 2):S50-57. https://doi.org/10.1111/j.1525-1497.2006.00363.x.
77. Simon SR, Kaushal R, Jenter CA, et al. Readiness for electronic health records: comparison of characteristics of practices in a collaborative with the remainder of Massachusetts. *Inform Prim Care*. 2008;16(2):129-137. https://doi.org/10.14236/jhi.v16i2.684.
78. Adjerid I, Adler-Milstein J, Angst C. Reducing Medicare spending through electronic health information exchange: the role of incentives and exchange maturity. *Info Syst Res*. 2018 (forthcoming).

Funding/Support: This work was supported by a grant from Stanford University's Cybersecurity Initiative. All views expressed are those of the authors only.

Conflict of Interest Disclosures: All authors have completed and submitted the ICMJE Form for Disclosure of Potential Conflicts of Interest. No conflicts were reported.

Acknowledgments: The authors thank Allen Briskin for helpful background information and Lorene Nelson for helpful comments on an earlier draft of the manuscript.

Address correspondence to: Michelle Mello, Stanford Law School, 559 Nathan Abbott Way, Stanford, CA 94305 (email: mmello@law.stanford.edu).