Bloomberg BNA

BNA's
Health Law Reporter™

Realizing the Potential of Health Information Exchange

By Steve Gravely and Erin Whaley

INTRODUCTION

The health care system is undergoing yet another evolution. Recognizing the need for change, health care providers and payers are fundamentally changing the manner in which health care is provided. This is extremely difficult in our fragmented health care system. More timely access to complete and accurate clinical information about patients is almost universally accepted as one component of a more efficient and effective health care system. There are substantial legal and operational barriers, however, to successfully implementing this vision. Health information exchange organizations (HIEOs) are one solution. While the technology exists to enable the rapid sharing of electronic health information, the legal and regulatory obstacles remain significant. This article discusses the principal legal and regulatory issues that confront HIEOs and how those can be managed.

Steven D. Gravely is the Health Care Practice Group Leader for Troutman Sanders. He focuses his practice in the area of health law and has represented hospitals and other health care providers for over 20 years. He can be contacted at steven.gravely@troutmansanders.com.

Erin S. Whaley is a partner in the Health Care Practice Group at Troutman Sanders. She represents hospitals and other health care providers in a variety of health care legal issues. She can be contacted at erin.whaley@troutmansanders.com.

SETTING THE CONTEXT

As the U.S. Supreme Court considers the constitutionality of the Patient Protection and Affordable Care Act (ACA),[1] the debate about health care reform rages on. The Supreme Court's ruling will have a profound impact on the shape of this debate and, ultimately, on the future of health care in America. Most observers, however, agree that regardless of how the court rules, the health care system already is reforming itself. Large health plans already have announced that they are moving ahead with implementation of key provisions of the ACA even if the court rules that some, or all, of the law is unconstitutional.[2] Pursuing the ''triple aim'' of lower costs, higher quality, and better access to care is at the top of most health systems' agendas.[3] The health care marketplace is driving this change and everyone who is involved in the delivery of health care or the payment for health care services is responding.

It is a truism that the American health care delivery system is fragmented. ''Care coordination'' and ''Patient centered medical home'' initiatives are being developed across the county in the hope that some of this fragmentation can be eliminated. A consequence of the fragmented health care delivery system is that vital clinical information about patients also is fragmented and is not accessible by physicians and other caregivers who need it. Having better access to more timely clinical information about patients is considered critical to achieving the ''triple aim'' simply because information

[1] Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010).

[2] Both UnitedHealthcare and Humana issued press releases recently affirming that their plans will implement key provisions of the act regardless of how the Supreme Court rules.

Humana to Voluntarily Preserve Key Health Care Reform Protections, available at http://press.humana.com/news/humana/20120611006392/en/Humana-Voluntarily-Preserve-Key-Health-Care-Reform (last accessed June 12, 2012).

UnitedHealthCare Voluntarily Extends Important Health Reform Protections Regardless of Upcoming Rulings by Supreme Court, available at http://www.uhc.com/news_room/2012_news_release_archive/health_reform_protections_to_be_extended.htm (last accessed June 12, 2012).

[3] Maureen Bisognan and Charles Kenney, *Pursuing the Triple Aim: Seven Innovators Show the Way to Better Care, Better Health, and Lower Costs* (2012).

 ISSN 1064-2137

is critical to the delivery of care. This is exactly why health care providers, payers and other stakeholders are coming together using an interesting variety of legal structures to develop HIEOs. While the digitization of health data has created the technical ability to share clinical data across information systems in ways that, until recently, have been impossible, the great excitement of achieving widespread health data exchange has been tempered by the tremendous complexities of developing a viable and sustainable HIEO.

LEGAL COMPLEXITIES OF HEALTH INFORMATION EXCHANGE

Health information exchange is a recent business activity within the complicated health care delivery system. Like most activities in health care, health information exchange must be done within the confines of an intricate web of state and federal laws governing the privacy and security of health information and relationships among those involved in the delivery of health care. All too often, these laws, some of which still are evolving, are seen as insurmountable barriers which are at odds with the very nature of health information exchange. However, they need not be obstacles to the development of HIEOs.

This article will provide a brief overview of key federal laws that govern health information and those who use, store, access, or transport that information. Only a brief summary of these very complicated laws is possible in this article, but it should provide a perspective for the larger context in which HIEOs operate.

HIPAA

The privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[4] and the accompanying privacy rule[5] and security rule[6] impose legal obligations on covered entities and their business associates related to how they use and disclose protected health information (PHI). HIPAA essentially establishes a minimum national standard for the protection of PHI. The requirements of the HIPAA privacy and security rules are well known at this point. Covered entities and business associates have adopted comprehensive business practices to assure that PHI only is used and disclosed in compliance with those rules. Covered entities may use and disclose PHI for treatment, payment, and health care operations, as defined by HIPAA (collectively referred to as TPO), without an authorization from the individual. Disclosure of PHI beyond TPO requires the patient's authorization unless one of the specifically enumerated exceptions applies. Disclosures for TPO typically are very important to HIEOs since these three reasons form the foundation of the vast majority of health information exchange initiatives.

It is important to understand that the privacy rule primarily addresses the ''use'' and the ''disclosure'' of PHI and the rights of individuals to their own PHI. It does not prohibit the electronic exchange of PHI, the use of electronic medical records, nor does it prohibit covered entities from participating in HIEOs as long as there is an enforceable legal framework to assure that the PHI is being exchanged in compliance with HIPAA. Some attorneys, privacy officers, and security officers believe that HIEOs cannot be developed and operated in compliance with HIPAA requirements. Such opinions usually are based on old or incomplete information and certainly do not reflect current thinking on this issue. Indeed, there are many operational HIEOs in 2012 that are in compliance with HIPAA and other federal laws. The fear of noncompliance with HIPAA never should be a reason not to develop an HIEO.

HITECH

Enacted as part of the ACA, the Health Information Technology for Economic and Clinical Health (HITECH) Act [7] makes every HIEO a business associate of the covered entities that transact PHI through the exchange. The effect of this is to extend the applicability of the HIPAA privacy and security rules to HIEOs. Importantly, HITECH does not make HIEOs covered entities under HIPAA. As a result, HIEOs are not required to directly support the individual rights provisions of the privacy rule. They can support these rights indirectly by providing any required information to the covered entity and allowing the covered entity to maintain the direct relationship with the individual. This is critically important since most HIEOs do not have a direct relationship with individuals and do not have the infrastructure required to respond to requests for access or amendment from individuals. As business associates, however, HIEOs are required to comply with most of the substantive requirements of the security rule.

HITECH also substantially expanded the requirements for the reporting of possible data breaches and increased penalties for data breaches. HIEOs must develop and implement mechanisms to detect and respond to data breaches including data breach reporting in compliance with HITECH and applicable state law. This should include a requirement that all HIEO participants report data breaches that could jeopardize the integrity of the HIEO network or call into question the safety and security of data that has been exchanged.

SAMHSA, Part 2 Records

The Substance Abuse and Mental Health Services Administration (SAMHSA) is the federal agency responsible for the oversight of federally assisted mental health and substance abuse treatment centers. These treatment centers provide a range of health care services and can be either free-standing or hospital-based programs. Many federally assisted substance abuse and mental health treatment centers are affiliated with community health centers. SAMHSA's ''Part 2'' regulations protect the confidentiality of alcohol and drug abuse records that would identify an individual as an alcohol or drug abuser when those records are obtained, created, or maintained by a federally assisted alcohol or drug abuse program for the purpose of treating alcohol or drug abuse, making a diagnosis for that treatment, or making a referral for that treatment.[8] The Part 2 rules are extraordinarily restrictive about the disclosure of these records. The restrictions, which follow the record

[4] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[5] 45 C.F.R. §§ 160, 164 (2003).
[6] 45 C.F.R. §§ 160, 164 (2003).
[7] American Recovery and Reinvestment Act, 42 U.S.C. §§ 17921, 17931-17932 and 17934 (2009).
[8] 42 C.F.R. § 2 (1973).

  HLR ISSN 1064-2137

in many circumstances, are so strict that the records cannot even be disclosed for treatment purposes without the individual's authorization (except in an emergency). Subject to specific enumerated exceptions, including a medical emergency, records covered by Part 2 only can be disclosed with a written authorization signed by the patient that identifies the specific records to be disclosed, the reason for the disclosure, the person making the disclosure, and the person to whom the disclosure is being made.

SAMHSA has issued FAQs to clarify how Part 2 records can, and cannot, be disclosed in an HIEO.[9] Unfortunately, SAMHSA has taken a very restrictive view of the Part 2 rules. By way of example, the SAMHSA FAQs clarify that the Part 2 authorization must include the names of individuals or organizations that will be receiving the records and cannot simply refer to an online list of HIEO participants. This is contrary to the entire model of a ''one to many network'' in which data is available to authorized participants when the data is related to one of the HIEO's permitted purposes.

A recent study by the Colorado Regional Health Information Organization included a finding that under existing Part 2 rules, it is effectively impossible to transact any information containing substance abuse records through an HIEO.[10] HIEOs must decide how they will address the exchange of records governed by Part 2 either by excluding all Part 2 records from the HIEO or developing some mechanism to comply with the rigid Part 2 requirements.

To the extent that Part 2 records will be exchanged through the HIEO, the HIEO likely will become the Part 2 service provider's qualified service organization (QSO). Being a QSO of a Part 2 provider is similar to being a business associate of a covered entity. There are, however, some very important, and at times conflicting, responsibilities of business associates and QSOs. HIEOs that are both business associates and QSOs will need to be mindful of their obligations in each type of relationship and have mechanisms in place to fulfill these obligations.

The Privacy Act of 1974

In addition to HIPAA, federal agencies are covered by the Privacy Act of 1974, [11] which prohibits disclosures of records contained in a system of records maintained by a federal agency (or its contractors) without the written request or consent of the individual to whom the record pertains. As with many of the other privacy laws, there are various statutory exceptions to this general rule. The Privacy Act also permits federal agencies to disclose information for other purposes by identifying the disclosure as a ''routine use'' and publishing notice of it in the *Federal Register*.

The Privacy Act's requirements on federal agencies can be more restrictive than those in the private sector. This can present unique challenges for HIEOs that desire to exchange information with federal agencies such as the Social Security Administration and the Department of Veterans Affairs . Both of these agencies are pioneers in the electronic sharing of health information and have successfully navigated the requirements of the Privacy Act to be able to engage in electronic health information exchange to support their respective missions.

FISMA

Federal agencies face much stricter security standards for their data systems than those imposed under the HIPAA security rule. The Federal Information Security Management Act (FISMA)[12] imposes an extremely rigorous security regimen on all federal information systems and all who have access to such systems. Importantly, FISMA does not extend beyond the federal agency information system. As a result, HIEOs or other private parties that do not have direct access to a federal agency information system do not have to comply with FISMA.

State Privacy and Security Laws

A survey of state laws protecting the privacy and security of health data is beyond the scope of this article. Some states have enacted a comprehensive set of laws and regulations that govern health information exchange and HIEOs specifically or that impose specific requirements in addition to HIPAA for the privacy and security of health information generally. Most states have adopted laws that provide greater protections than HIPAA for specific types of information that are considered particularly sensitive. These usually involve behavioral health information, sexually transmitted disease information, records of minors, and, in some states, genetic information. Most states also have enacted laws or regulations that require suspected data breaches to be reported to one or more state agencies. The state data breach reporting requirements are in addition to any federal reporting requirements under the HITECH Act.

HIPAA provides that if a state privacy law provides greater protection than HIPAA, then the state law controls and is not preempted by HIPAA. Under the HIPAA preemption provisions, therefore, these more protective state laws govern, even though they go beyond the HIPAA requirements. This can present significant challenges to the development of HIEOs especially those that cross state lines. If you are planning to develop an HIEO, you must check the laws of each state in which you plan to operate to identify state specific laws that will apply to the HIEO and to the health information that is being exchanged.

Other Relevant Laws

When lawyers and their clients consider the legal issues associated with developing an HIEO, they usually focus on federal and state laws and regulations related to privacy and security. There are other laws and regulations that will apply to those developing an HIEO,

[9] Sarah Wattenberg, *Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange*, Substance Abuse and Mental Health Services Administration, available at http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf (last accessed June 12, 2012).

[10] *Supporting Integration of Behavioral Health Care Through Health Information Exchange: Recommendations for Integrating Colorado's Mental Health, Substance Use Treatment, and Medical Communities through the Development of Statewide HIE*, Colorado Regional Health Information Organization, available at http://www.corhio.org/media/40757/supporting_integration_of_behavioral_health_care_through_hie_april_2012-web.pdf (last accessed June 12, 2012).

[11] 5 U.S.C. § 552a (1974).

[12] 40 U.S.C. 11331, 15 U.S.C. 278g-3 & 4 (2002).

most importantly federal tax law and laws relating to ''fraud and abuse.''

Tax Exempt or Not?

An HIEO must decide if it will seek tax exempt status from the IRS. Some HIEOs have sought tax exempt status under IRC section 501(c)(3) with mixed results. As HIEOs are a relatively new phenomenon, the IRS has carefully considered their applications for tax exempt status resulting in long delays in the review and approval process. Recently, the IRS has acknowledged that HIEOs that are organized and operated to facilitate health information exchange can qualify for 501(c)(3) status. Specifically, the IRS noted, ''Congress recognized that facilitating health information exchange and technology is important to improving the delivery of health care and reducing the costs of health care delivery and administration. The legislative history of [the American Recovery and Reinvestment Act of 2009] acknowledges that certain organizations that are organized and operated to facilitate the exchange of health information, and that satisfy standards established by Health and Human Services, lessen the burdens of government and may qualify for exemption under section 501(c)(3).''[13]

If the HIEO is not going to seek tax exempt status from the IRS, but has members that are tax exempt, the HIEO will have to consider the exempt status of these members when designing its governance structure. For instance, if the HIEO is owned by a combination of for-profit and tax exempt providers, the tax exempt providers likely will require a greater degree of control in the governance of the HIEO to ensure that the HIEO is operated in accordance with the member's tax exempt purposes. These types of requirements typically serve to complicate the governance discussions, which already are complicated enough.

Fraud and Abuse Laws

HIEOs usually involve a combination of hospitals, health systems, and physicians who are investing different amounts of money, time, energy, and talent. Where physicians, who have the ability to control referrals to hospitals and health systems, have a governance interest that exceeds their invested equity, however, there could be a potential unjust inducement or remuneration that would implicate the federal Stark or anti-kickback laws.[14] This is an extremely complicated analysis that depends entirely on the facts and circumstances of each case. However, lawyers who are advising HIEOs must analyze the structure and consider whether any improper inducements or remuneration exist.

THE CHALLENGE FOR HIEOs

The complex body of federal and state laws summarized in this article was created over many years to preserve the confidentiality of a patient's health records, to regulate who can become a tax exempt organization, and to prevent fraud and abuse in the delivery and payment of health care services. Today, these laws create an overlapping, and sometimes inconsistent, legal environment that makes it difficult to understand exactly what set of rules apply to an HIEO. A major challenge faced by HIEOs has been finding a way to employ the technology that is available to exchange health information electronically in compliance with all of the relevant legal authority and structuring it in a way that does not violate the Stark or anti-kickback laws.

This is much more complicated than it may sound since none of the statutes or regulations referenced here were written with the electronic exchange of health information in mind. Lawyers and other advisers are left to interpret existing law and predict how those laws will be applied to the world of electronic health information exchange without the benefit of any definitive guidance from either the courts or the federal government. The complexity of these laws and the lack of definitive guidance create an environment in which attorneys and their clients must superimpose their own risk tolerances in determining how to comply with the applicable laws. The result is quite a bit of variance across the country in how these laws are interpreted and applied. Experienced health care lawyers encounter this type of variability often, but it is particularly challenging when establishing an HIEO. This is because developing a consensus about the privacy and security ''rules of the road'' that will apply to all the participants in the HIEO is critical to creating a viable trust framework that will support robust exchange.

Early efforts at developing HIEOs, in the early 2000s, pursued a ''least common denominator'' approach in which the strictest interpretation of any of the stakeholders was adopted as the *de facto* standard. This approach stymied HIEO development activity since it imposed unmanageable restrictions on all the participants and resulted in very little health data being transacted at a relatively high cost. HIEOs continue to struggle with this issue today. It is vital that HIEOs not adopt a ''least common denominator'' approach in order to engage every stakeholder. While this might mean that some stakeholders will not participate in the HIEO initially, it is likely that they will decide to join once the HIEO has begun data exchange and has demonstrated that it can do so safely and securely.

The very real legal risks that face HIEOs require tools that help to mitigate the risk. One of the most widely accepted tools is a comprehensive trust agreement among all of the participants in the HIEO that will set forth the mutual expectations and obligations of everyone who participates in the HIEO. While ''point to point'' data sharing agreements have existed for a long time, HIEOs require a fundamentally different type of trust agreement. A part of the development of the Nationwide Health Information Network (NHIN) was the drafting of the Data Use and Reciprocal Support Agreement (DURSA), a first-of-its-kind multi-party trust agreement to support nationwide data exchange among nonfederal HIEOs and federal agencies. The DURSA was developed through a multi-stakeholder work group that was funded by the Office of the National Coordinator for Health Information Technology (ONC) as part of the NHIN Trial Implementation Phase 2. The DURSA broke new ground in addressing the complex legal issues related to data exchange. While the DURSA is being used as a template by HIEOs across the country to help them develop their own trust documents, it should not simply

[13] *What triggered the increased public interest in RHIOs?* Internal Revenue Service, available at http://www.irs.gov/charities/charitable/article/0,,id=206124,00.html (last accessed June 14, 2012).

[14] 42 U.S.C. § 1395nn (2007).
42 U.S.C. § 1320a-7b (1987).

   ISSN 1064-2137

be adopted in whole. It should be customized to address each HIEO's specific policy and technical infrastructure.

The complicated legal environment for HIEOs continues to become even more complicated. On May 15, 2012, ONC issued a request for information (RFI) seeking public comment on a proposed framework for a governance mechanism for the NHIN. In 2009, Congress mandated that ONC ''develop a mechanism for governance of the Nationwide Health Information Network.''[15] Since that time, ONC has convened multiple workgroups and has obtained input from the HIT Policy Federal Advisory Committee on governance models that would be relevant for the NHIN.

The RFI includes a complex framework that calls for HIEOs to become certified as NHIN validated entities (NVEs). While voluntary at this point, the RFI makes clear that NVE status might well become a requirement for contracting with federal agencies or might become a requirement for other critical initiatives. In order to become an NVE, an organization must comply with a range of conditions for trusted exchange (CTE). The CTEs are grouped in three categories in the RFI: safeguards, interoperability, and business practices. There are 10 CTEs under the safeguard category, three under the interoperability category, and three under the business practices category. In order to become certified as an NVE, an organization must comply with all of the CTEs, not only some of them. The RFI has generated considerable discussion in the health care industry and it is expected that there will be a large number of comments submitted prior to the deadline on June 29.

Considering the very complicated state and federal laws and regulations affecting health information exchange, it is notable that HIEOs have developed at all. The federal funding applied to health data exchange, while substantial, has not approached the actual cost of developing an HIEO. Those ventures that relied solely on federal funding have mostly failed unless they succeeded in finding private funding. New HIEO projects are nearly all privately funded. This reflects a genuine consensus that having timely and complete information in the hands of caregivers, care managers, payers, and others that are involved in the health care industry will help to reduce unnecessary services, duplicative tests, and delays in treatment that both increase costs and put the patient at risk for complications and other adverse outcomes.

The digitization of health records has created the technical opportunity for health information to be exchanged electronically. The existing complex legal environment that was designed to protect the confidentiality of health information has hindered the development of HIEOs and has complicated the development of consensus among health care stakeholders and their attorneys on the best practices for sharing patient data through an electronic community. Even forming the legal entities that will house the health information exchange activity is complicated by the byzantine requirements of the Stark, anti-kickback, and tax exempt entity laws.

The complex legal and regulatory framework within which HIEOs operate is very dynamic and will continue to evolve for the foreseeable future. It is likely that there will be some type of governance framework established for the NHIN. The exact contours of that governance framework are yet unknown but will affect the way in which HIEOs operate and the cost of that operation. Health care reform is happening and will continue regardless of how the Supreme Court rules. The need to lower costs, improve quality, and enhance access to care is not going away.

Admittedly we live in a complex world. Unfortunately, the complexity presented by these important federal and state laws has too often become an excuse for not moving forward with HIEO development. This does not have to be the case, since these laws do not prohibit the formation of HIEOs. There are success stories where HIEOs have overcome these barriers through concerted efforts and perseverance. It is not easy, but the very fact that health care providers, payers, and others have been willing to commit the significant time, energy, and money to develop operational HIEOs in such a hostile environment is a testament to the fact that there is a compelling need for health data exchange. Only with reliable and accessible electronic health information exchange can the ''triple aim'' of lower cost, higher quality, and better access be achieved in an effort to truly reform our health care delivery system.

[15] 42 U.S.C. § 300jj-11 (2009).