All HIEs Are Not Created Equal: Privacy and Security Considerations Related to HIE Participation

Holly Carnell
John Saran
McGuireWoods LLP
Chicago, IL

A health information exchange (HIE) enables health care providers to securely access and share a patient's medical information electronically. Thus, HIEs have the ability to improve the quality of health care delivery by coordinating care among otherwise-unaffiliated providers, resulting in many benefits, including improved patient safety, reduced frequency of medical errors and duplicated tests, and overall increased efficiency. In addition, HIEs may help health care providers meet meaningful use measures with the provider's electronic health record (EHR) under the Medicare and Medicaid EHR Incentive Programs. Specifically, health care providers can use data transmission through HIEs to fulfill their public health reporting and care coordination requirements of these programs to receive Medicare and Medicaid financial incentives.

This article provides background on HIE models and the applicability of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA)[1] to all health information organizations (HIOs) that operate HIEs. This article also offers seven privacy and security considerations for HIE participation. Ultimately, a health care provider must realize that an HIO must balance its desire to be user friendly and self-sustaining with its obligations of appropriately safeguarding (and requiring other participants to appropriately safeguard) the protected health information (PHI) of its participants.

HIE Models

In 2009 the Office of the National Coordinator for Health Information Technology (ONC) was established in law by the Health Information Technology for Economic and Clinical Health (HITECH) Act.[2] ONC is responsible for the administration of HITECH state cooperative agreements that provide grants to state-designated HIOs to develop HIEs. However, with the grant funding period expiring, HITECH funding for state-run HIEs may not be available past 2014 or early 2015.[3] As a result, state HIOs must secure state or supplemental federal funding or become fully self-sustaining through the assessment of participation fees on participants.[4]

HIEs come in various shapes and sizes and can be run by public agencies, health care providers, payers, and public-private partnerships. However, HIOs generally utilize one of two core HIE models (or a hybrid of the two): a centralized model or a federated model. The centralized model involves the HIE acting as a data repository that collects data from its participants and stores it in a central data repository.[5] HIE participants can then access, download, and update PHI according to defined policies and procedures. The federated model differs in that the HIE acts as an intermediate facilitator for locating and exchanging data between participants; in this

model, patient data is only populated in the EHR systems of the individual participants and is accessed and exchanged only when queried by the HIE on behalf of another participant.

While the centralized model provides for faster response times to queries and the ability to perform data analytics, it requires a substantial investment in network capability.[6] Furthermore, a central data repository runs a greater risk of data duplication and incorrect record matching and provides hackers or other unauthorized users with a central entrance point. Conversely, a federated model comprising several repositories at the provider level would require a hacker or unauthorized user to separately query the data repositories of individual participants to access the data of all the HIE participants. The federated model's reliance on individual EHRs isolates defects and system failures, but does not guarantee fast response times or complete data availability.

HIPAA Applicability

On January 25, 2013 the U.S. Department of Health & Human Services (HHS) published the Omnibus Final Rule (Omnibus Rule) interpreting and implementing various provisions of the HITECH Act and the Genetic Information Nondiscrimination Act of 2008. The Omnibus Rule amended the definition of "business associate" to specifically include HIOs.[7] Further, the commentary to the Omnibus Rule discusses the difference between HIOs and data transmission organizations that do not require access to PHI on a routine basis and thus would not be considered a business associate. HHS noted:

> In contrast, an entity that requires access to [PHI] in order to perform a service for a covered entity, such as an [HIO] that manages the exchange of [PHI] through a network on behalf of covered entities through the use of record locator services for its participants (and other services), is not considered a conduit and, thus, is not excluded from the definition of business associate.[8]

Following the HITECH Act and the Omnibus Rule, there is little room for argument that an HIO is not a business associate, and even HIOs utilizing the federated HIE model will not be able to rely on the "mere conduit" exception. HHS declined to define the term "HIO" because it recognized that the industry was rapidly evolving, and did not want to limit the definition.[9] HHS indicated that it will publish guidance regarding entities that fall within and outside the HIO definition as the industry continues to evolve.[10] Under the HITECH Act, business associates, including HIOs, are directly liable to the federal government for noncompliance with certain provisions of the Privacy and Security Rules, and are subject to the Breach Notification and Enforcement Rules. The application of HIPAA to business associates imposed compliance obligations, and the risk of substantial civil and criminal penalties for noncompliance on HIOs.

Seven Privacy and Security Considerations Related to HIE Participation

A health care provider's participation in an HIE may create increased risk with respect to the privacy and security of the PHI of the provider's patients. This increased risk is in part a result of the significantly increased number of individuals who have access to the health care provider's PHI, most of whom are not members of the workforce of the provider, i.e., the provider has limited control over most of the individuals who will have access to the provider's PHI. A health care provider instead has to rely on the HIO operating the HIE and the other participants' safeguards to protect the PHI of its patients stored by or available through the HIE. Consistent standards applied to the HIE, and its participants, can facilitate the efficient exchange of information and help foster trust among participants and patients.

The Privacy Rule allows covered entities participating in an HIE to agree on a common set of privacy safeguards that are appropriate to the risks associated with exchanging PHI through the HIE.[11] Overly prescriptive safeguards could cause health care providers to seek alternative mechanisms for data transfer, while broad and nonspecific delegation of responsibility will likely not engender trust in the HIO's approach. Thus, HIOs must strike a balance of requiring participants to implement reasonable safeguards with mechanisms to remediate issues, remove noncompliant participants, and appropriately allocate liability. In addition, it is important that the permitted uses and disclosures of PHI are specifically described.

Following are seven privacy and security considerations for health care providers when assessing HIE participation agreements provided by public, private, or payer HIOs.

Privacy and Security Safeguards

As a business associate, an HIO has numerous compliance requirements under HIPAA. These requirements include achieving and maintaining full compliance with the Security Rule. Further, a business associate is required to notify its covered entity clients, in this case HIE participants, within a specified statutory timeframe in the event of a breach of unsecured PHI. A business associate also is required to comply with certain provisions of the Privacy Rule. HIOs must enter into a business associate agreement with each covered entity participant, which should outline these responsibilities. A health care provider should ensure that the HIE participation agreement includes a compliant business associate agreement and should perform diligence on the HIO's HIPAA compliance. A participant also may attempt to retain audit rights with respect to documentation supporting the HIO's compliance with HIPAA.

Accountability: Breach Mitigation and Allocation of Liability

HIOs face complex issues in coordinating breach notification and mitigation responsibilities among themselves and the

HIE participants. Pursuant to HIPAA, a covered entity has the responsibility to notify an affected individual (in this case, a patient) of a breach without undue delay but in no event later than 60 days from discovery,[12] and the covered entity must, to the extent practicable, mitigate any known harmful effects of the breach.[13] However, an HIE is often composed of diverse participants including other HIEs.[14] Absent straightforward protocols, disorder may ensue over who is responsible for notifying affected individuals and incurring the costs of mitigation. For example, it may be unclear which provider participant must notify a particular patient of a breach where multiple providers have a treatment relationship with the patient. Similarly, an individual would likely be confused by the receipt of a breach notification from multiple parties. HHS has provided guidance with respect to breach notification in an HIO context.[15] Specifically, HHS suggests that when multiple covered entities participate in an HIE and there is a breach, it may be necessary for the HIO to notify all potentially affected covered entities and for those covered entities to delegate to the HIO the responsibility of sending the required notifications to the affected individuals.[16]

Some HIOs develop breach policies in collaboration with representatives of their participants. By ensuring that participants are engaged in the development of policies and protocols, not only does the HIO benefit from the collective knowledge of participants, but also the end result is more likely to be acceptable and desirable to participants. Participants should be aware that while the contractual duty to mitigate harm resulting from a breach may be allocated to the participant that causes the breach, certain participants may not have the resources to fully mitigate the harm caused by a large breach. Certain HIOs have attempted to remedy this issue by requiring that all participants obtain insurance coverage for this purpose. Health care providers should consider such coverage regardless of contractual obligations and assess whether the HIO itself has sufficient insurance coverage and resources to mitigate a breach.

Scope and Limitations of Permissible Uses and Disclosures of PHI

HIOs must determine the scope of permissible uses and disclosures of PHI by participants. Except for purposes of treatment and certain other narrow exceptions, HIPAA requires that the use or disclosure of PHI is limited to the minimum necessary to accomplish a specific purpose.[17] While HIPAA provides a floor in terms of permissible uses and disclosures, an HIO may impose more-restrictive standards with respect to uses and disclosures by HIE participants. Often, HIOs will utilize the HIPAA definitions of "treatment," "payment," and "health care operations" in establishing the permitted uses and disclosure of PHI by HIE participants. An HIO also will often require permission to use PHI from its participants for various purposes related to the HIO's management of the HIE, for example, maintaining a master patient index for linking information about a particular individual. Participants should determine whether the HIO intends to use PHI originating from HIE participants for the purposes of research, analytics, or public health reporting and, if so, the parameters of these activities. Further, as discussed below, state law also may necessitate restrictions on uses and disclosures. Health care providers should ensure the delineated uses and disclosures of PHI are acceptable (both in terms of applicable law and organizational requirements) and that its patients are put on notice of these uses and disclosures (*see* Patient Communication) and that other participants also are required to ensure their patients are provided with such notice.

Openness and Transparency: HIE Governance

HIOs face the challenge of developing a unified form of participation agreement with individual providers that often desire to negotiate unique agreements. A fluid negotiation process for every participation agreement could yield hundreds of different sets of privacy and security obligations between the HIO and its participants, which could become unwieldy and impossible to monitor. To mitigate this issue, some HIOs engage stakeholders (which may include participants and otherwise-interested nonparticipants, such as patient rights advocates) to help develop policies and procedures that are mandatory for all participants. Health care providers should be cognizant of an HIO's consideration of stakeholder input into its policies and procedures and of opportunities for stakeholder involvement in decision making. For example, the Illinois Health Information Exchange (ILHIE) Authority addressed the breach notification and mitigation quagmire by adopting a standard policy and procedure. The ILHIE Authority initiated a committee process to develop a detailed plan in the event of a breach with the input of various health care providers, regional HIOs, health plans, and individual rights advocates in Illinois. The end result was a standard for coordinating breach investigation, mitigation, and notification efforts, which became a nonnegotiable condition for participation.

Individual Choice

Health care providers should be aware of the HIO's patient participation models. The most-common consent models are the opt-in and opt-out models, while providers also have the option to include all of a patient's PHI without obtaining specific consent. Further, some HIOs elect to add conditions to the opt-in or opt-out model. By 2012, 27 states had adopted some form of the opt-out model, while 12 states selected the opt-in model.[18] In the opt-in model, the provider must obtain consent from a patient before exchanging that patient's PHI on an HIE. Conversely, the opt-out model automatically enrolls patients in the HIE, but the patient must be given the opportunity not to participate.[19] If a patient opts out of the exchange, then the patient's entire record would be restricted from the HIE. As technology continues to develop, more HIOs may be able to grant patients the ability to opt in or out with respect to a subset of their information. Participants should understand the HIO's consent model and ensure it has the technical and procedural means to comply with the HIO's requirements and to communicate the model to patients. Moreover, to the extent a participant desires to use a more-

stringent consent requirement than the HIO, the participant should ensure that the use of such consent process does not violate the HIO's conditions of participation.

Patient Communication

Health care providers looking to foster trust in the secure use of HIE technology can communicate with patients about its participation in an HIE. As a business associate, HIOs do not need to provide individuals with a notice of privacy practices. Rather, that obligation falls to the covered entity that has a direct relationship with the patient.[20] The HHS Office for Civil Rights Guidance indicates that health care providers could incorporate into their non-physician providers notice of HIE participation, permitted uses and disclosures via the HIE, and explain how the HIO maintains a private and secure network. With knowledge of the health care provider's participation in an HIE, individuals might be more willing to choose to obtain services from the health care provider, especially if the individual's other health care providers participate in the same HIE.[21] Additionally, this notice of disclosures and privacy and security measures could be used in conjunction with implementing the HIO's consent model to better inform the patient's choice.[22]

State-Specific Restrictions

Health care providers also should consider state law privacy barriers that could affect HIE participation. HIPAA generally preempts state law, unless the state law is more restrictive than HIPAA.[23] Typical state law restrictions that go beyond HIPAA include laws governing genetic information, mental health records, substance abuse records, human immunodeficiency virus records, and informed consent. These restrictions could lead to entire records being excluded from HIEs, as data-aggregating software used by HIOs does not always have the capability to redact only the sensitive information. To combat these roadblocks, HIOs are working closely with vendors to make granular data restrictions on the display of sensitive information a reality. Parallel to these efforts, HIOs are engaging in lobbying and lawmaking efforts to soften certain state law restrictions that make HIE operation costly and burdensome. Providers should review applicable state law and ensure that the HIO has the capability to enable the provider to comply with state law and that the provider has appropriate protocols in place to identify elements of records that are subject to state restrictions.

Conclusion

When considering whether to participate in an HIE, a health care provider should understand how the HIE operates, including the privacy and security requirements imposed on the provider, the HIO and the HIE's other participants, and the enforcement and remediation mechanisms related thereto. Further, health care providers should understand the role of HIPAA and applicable state law with respect to the HIE and its participants. Finally, a health care provider should assess its comfort with the patient consent model and the level of participant input the HIO considers in its governance activities and development of policies and procedures.

---

1 Including what are commonly known as the Privacy Rule, the Security Rule, the Enforcement Rule, and Breach Notification Rule applicable to covered entities and business associates.

2 The HITECH Act was part of the American Recovery and Reinvestment Act.

3 Josh Israel and Kimberly Leonard, *Stimulus funds will build state health exchanges but might not sustain them,* Health Care IT News, Nov. 10, 2011, *available at* www.healthcareitnews.com/news/stimulus-funds-will-build-state-health-exchanges-might-not-sustain-them.

4 Anthony Brino, *HIE seeking answers to sustainability,* Health Care IT News, July 11, 2013, *available at* www.healthcareitnews.com/news/hies-seeking-answers-sustainability?page=0; these options do not apply for non-state-designated entities that operate HIEs, as such HIEs have to be self-sustainable; *see CMS Answers to Frequently Asked Questions*, HHS, Sept. 10, 2013, *available at* www.medicaid.gov/Federal-Policy-Guidance/downloads/FAQ-09-10-2013.pdf.

5 Healthcare Info. Mgmt. Sys. Soc'y, A HIMSS Guide to Participating in a Health Information Exchange 15-17 (2009), *available at* www.himss.org/files/HIMSSorg/content/files/HIE_GuideWhitePaper.pdf.

6 *Id.* at 17-19.

7 45 C.F.R. § 164.103.

8 Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under the [HITECH] and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 87 Fed. Reg. 5566, 5572 (Jan. 25, 2013) [hereinafter Omnibus Rule Commentary].

9 *Id.* at 5571.

10 *Id.*

11 *Does the HIPAA Privacy Rule allow covered entities participating in electronic health information exchange with a health information organization (HIO) to establish a common set of safeguards?*, HHS, Dec. 15, 2008, *available at* www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/571.html.

12 45 C.F.R. §164.404.

13 *Id.* § 164.530(f).

14 Certain issues may arise when an HIE is a participant of another, larger HIE because the larger HIE does not have privity of contract with the smaller HIE's participants. These issues include coordination of breach notification and the enforcement of data use restrictions.

15 *Omnibus Rule Commentary, supra* note 8, at 5651.

16 *Id.*

17 45 C.F.R. § 164.502(b)(1).

18 Three states did not require any kind of consent, while eight states still had not decided yet. Ill. Office of Health Info. Tech., Overview of Patient Consent Models 11 (July 22, 2012) [hereinafter ILHIE White Paper], *available at* www2.illinois.gov/gov/HIE/Documents/SNConsent%20Draft%207%2020%2012%20(2).pdf.

19 ILHIE White Paper, supra note 18, at 3-5.

20 45 C.F.R. § 164.520(a)(1).

21 HHS, Office for Civil Rights, *Privacy and Security Framework: Openness and Transparency Principle and FAQs* 2 [hereinafter *OCR Openness and Transparency Guidance*], *available at* www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/opennesstransparency.pdf. HHS does not consider paying for HIE services to be sale of PHI, and HIEs are likely not engaging in the practice, but the selling of PHI is not outside the realm of possibility as HIEs succumb to the market pressures of running a business. *Omnibus Rule Commentary, supra* note 18, at 5606.

22 *OCR Openness and Transparency Guidance, supra* note 21, at 3; HIPAA requires acknowledgement of receipt of a notice of privacy practices, which is different than informed consent by an individual to have his or her PHI participate in an HIE.

23 45 C.F.R. § 160.203.