BNA, INC.

HEALTH IT LAW & INDUSTRY

BNA Employee-Owned Since 1947

VOL. 3, NO. 31 AUGUST 1, 2011

Ten Key Privacy Issues for Health Information Exchanges

By Robert Belfort

Community-wide electronic health information exchanges (HIEs) are a centerpiece of current federal health care policy. HIEs are likely to play an important role in the development of accountable care organizations, the ''meaningful use'' of electronic health records under Medicare and Medicaid incentive programs and the implementation of a variety of other government initiatives to improve health care quality and control costs. Yet HIEs are still struggling to gain traction in many communities. There are several reasons for the uneven progress of HIEs , including the search for a viable business model and questions about appropriate governance structures. But chief among the challenges facing HIEs is the need to resolve thorny privacy issues. Ten of the top privacy issues commonly confronted by HIEs are discussed below.

Robert Belfort is a partner in the health law practice of Manatt, Phelps & Phillips, LLP. He is based in the firm's New York City office.

1. ***Patient Consent***. The Privacy Rule issued under the Health Insurance Portability and Accountability Act (HIPAA) permits health care providers and health plans to use and disclose protected health information (PHI) for treatment, payment and health care operations without patient consent.[1] These exceptions generally cover all or most of the transmissions of PHI made through an HIE. But state laws may impose more stringent patient consent requirements, especially with respect to sensitive information such as mental health and HIV records.[2] In addition, federal regulations require consent for the disclosure of records of federally assisted alcohol and drug abuse treatment programs.[3] Thus, depending on the state, HIEs are legally required

[1] 45 C.F.R. § 506(c).

[2] *See, e.g.*, N.Y. Mental Hygiene Law § 33.13 and N.Y. Public Health Law Article 27-F.

[3] 42 C.F.R. Part 2.

 ISSN 2151-2876

to implement a patient consent process for some or all of the information they transmit, unless all data subject to patient consent laws can be excluded from the HIE.

Moreover, even if patient consent is not legally required, it is often demanded by consumer groups and other stakeholders who believe that HIEs raise new privacy risks that warrant a heightened level of patient consent. When a patient consent process is driven by policy concerns rather than legal requirements, the options for managing the consent process proliferate. Among the issues for consideration by the HIE are (i) whether consent should be provided on an opt in or opt out basis, (ii) if an opt out consent process is utilized, what type of patient education will be provided about consent options, (iii) whether consent will be obtained by providers *disclosing* records through the HIE or *accessing* records through the HIE, (iv) how responsibility for collecting and tracking consents will be allocated between participants and centralized HIE staff, and (v) the extent to which patients can limit their consents to particular providers, types of information or dates of service. More than any other issue, patient consent tends to divide stakeholders into different camps that have varying views on the proper balance between protecting patient privacy and promoting the efficient operation of the health care system.

2. ***Minor Consent Services***. Most states authorize minors to provide informed consent for certain health care services without the consent of a parent or guardian. In many cases, information relating to these ''minor consent services'' is controlled by the minor. In other words, the minor, rather than a parent or guardian, must consent to the disclosure of this information. This regulatory framework presents significant challenges to HIEs, particularly those using an ''opt in'' consent model. If a parent provides consent for an HIE to exchange information about his or her child, that consent may not cover information relating to minor consent services. But the HIE is likely to have no means of distinguishing information controlled by the minor from information controlled by the parent unless the information controlled by the minor is filtered, tagged or segregated in some manner by the provider creating the records. And few providers appear to have the capacity to organize their records in this manner on a consistent basis. This problem frequently forces HIEs to consider a range of cumbersome options, such as obtaining consent from both the parent and minor for all disclosures of minors' records or excluding minors of a certain age from the HIE. Ultimately, the technical segregation of information relating to minor consent services in providers' record systems will likely be necessary to permit full participation in HIEs by minors without violating privacy laws.

3. ***Restriction on Disclosure Requests***. Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, patients have the right to restrict a provider from disclosing PHI about a particular service to the patient's health plan if the patient pays for the service out of pocket in full.[4] Proposed regulations have been issued by the U.S. Department of Health and Human Services (HHS) implementing this requirement.[5] These restriction requests raise a set of challenges for HIEs similar to those associated with minor consent services. If health plans participate in an HIE, provider records subject to a restriction request may unwittingly be made accessible to the patient's health plan unless these records can be separated from the rest of the patient's information. As is the case with information relating to minor consent services, the technical segregation of the restricted records in the provider's record system appears to be the optimal solution. But until this approach is universally feasible, HIEs will be searching for workarounds, most of which will be cumbersome.

4. ***Minimum Necessary***. The HIPAA Privacy Rule requires covered entities to use and disclose only the minimum necessary PHI for an authorized purpose.[6] The minimum necessary rule does not apply to the use or disclosure of PHI for treatment purposes.[7] But if an HIE facilitates the exchange of PHI for payment or health care operations, the minimum necessary rule is applicable. Providers disclosing PHI through an HIE are generally not in a position to make case-by-case determinations of which portion of their records is the minimum necessary for each access request by another provider. Fortunately, the Privacy Rule permits a disclosing covered entity to rely on the determination of the requesting covered entity that the PHI being requested is the minimum necessary.[8] But this approach imposes a duty on requesting providers to have some type of minimum necessary policy in place. In addition, reliance on the requesting party's determination is not permissible if this party is not a covered entity.

5. ***Research***. HIEs may provide a unique opportunity for researchers to efficiently gain access through a single source to large amounts of clinical data created by multiple provider organizations. Subject to certain exceptions, the HIPAA privacy rule permits the use and disclosure of PHI for research purposes without patient authorization only upon a waiver of patient consent granted by an institutional review board (IRB) or privacy board.[9] Historically, researchers have been required to seek the approval of the IRB or privacy board at each institution being requested to release PHI. The degree to which HIEs can serve as a more convenient source of data for research depends, in large part, on whether the IRB/privacy board approval process can be streamlined through the HIE. This streamlining will generally entail the creation of a ''super'' IRB or privacy board designated by the HIE to waive patient consent for research disclosures on behalf of all HIE participants. While HIPAA does not appear to restrict this approach, state laws may be more stringent. In addition, providers accustomed to controlling the use of their data for research through their own IRB may be resistant to ceding this authority to a ''super'' IRB designated by an HIE.

6. ***Commercialization of De-identified Data***. As they search for a viable, long-term business model to support their operations, some HIEs are considering the sale of de-identified data to commercial interests as a source of needed revenue. The HIPAA prohibitions on the sale of PHI do not apply to de-identified data.[10] Moreover, state laws that attempt to restrict the sale of

[4] HITECH § 13405(a).
[5] 75 Fed. Reg. 40868 (July 14, 2010).
[6] 45 C.F.R. § 164.502(b)(1).
[7] 45 C.F.R. § 164.502(b)(2)(i).
[8] 45 C.F.R. § 164.514(d)(1)(iii)(B).
[9] 45 C.F.R. § 164.512(i).
[10] 45 C.F.R. § 164.514(a).

  HITR ISSN 2151-2876

de-identified data by health care organizations are likely to be unconstitutional.[11] Nonetheless, HIEs and their participants may still be concerned about whether PHI is being properly de-identified. To meet HIPAA's test of de-identification, 19 specified identifiers must be removed from the PHI or a qualified statistician must provide an opinion stating that the risk of de-identification is very small.[12] Covered entities and their business associates, including HIEs, must employ safeguards to prevent re-identification. In addition to the privacy concerns raised by the de-identification of PHI, HIEs and their participants may also face policy questions about the types of commercial enterprises to which de-identified data should be sold and the purposes for which such enterprises may use the data.

7. ***Government Access***. Most HIEs envision sharing clinical data with government agencies for public health purposes. The disclosure of PHI to advance public health is permitted by HIPAA[13] and is expressly provided for in some state HIE laws.[14] There is rarely disagreement about the benefit of granting public health authorities access to HIE networks. But discussions about government officials gaining access for other purposes tend to be more contentious. Potentially, HIEs could be a source of useful information for health fraud investigators, licensing bodies and law enforcement authorities. But it is unclear to what extent granting these types of government agencies access to data is consistent with the expectations or the desires of providers or patients. While the HIPAA privacy rule may permit many of these disclosures, the rule does not require them. And state laws generally do not impose disclosure mandates on HIEs. As a result, the authority of an HIE to make these disclosures is usually a policy decision.

8. ***Subpoenas and Discovery Requests***. Many states have privilege statutes that shield medical records from discovery in civil litigation. But these statutes generally apply to records maintained by physicians, hospitals or other health care providers. The statutes do not contemplate HIEs. In resisting subpoenas and other discovery requests, HIEs will usually rely on the argument that they are maintaining data on behalf of providers, and that the electronic records in any HIE computer system are no more subject to discovery than the paper records stored by a provider in a warehouse. The strength of this argument may depend, though, on whether the HIE operates as a pure data custodian of its participating providers or patients actually authorize the disclosure of their records by providers to the HIE.

9. ***Patient Access***. Most HIEs are initially focused on facilitating data exchange among providers and health plans. But as HIEs develop, they may face increasing pressure to establish mechanisms for *patients* to access their records through the HIE. Indeed, the ability of patients to access all of their medical records from multiple providers through a single source may be one of the primary selling points in generating patient buy-in for HIEs.

The creation of a patient portal or other mechanism for patient access, however, raises a distinct set of privacy issues. HIEs must develop a reliable system for authenticating patient identity to ensure that imposters do not gain access to a patient's records. Most single-provider patient portal systems rely on an in-person contact between the provider and patient for authentication purposes. Providers participating in an HIE will have to accept broader responsibility to perform the authentication function unless the HIE establishes an alternative system.

In addition, the restrictions on the disclosure of information relating to minor consent services become even more sensitive in connection with a patient portal. While the disclosure of this information to a provider without the minor's consent may be inconsistent with law, it generally does not cause harm to the minor. In contrast, the inadvertent provision of access to this information to a minor's parent through a patient portal may have severe adverse consequences. As a result, segregating information relating to minor consent services is especially critical when a patient portal becomes available.

Finally, certain providers, especially those delivering mental health or other sensitive services, may prefer to review and potentially redact records before making them available to the patient, as is permitted by the HIPAA Privacy Rule and some state laws.[15] There may be challenges integrating this type of screening process into an HIE's patient portal.

10. ***Responsibility for Privacy Violations***. HIEs create a heightened level of interdependence among health care organizations. In some HIE models, providers obtain patient consent for the release of other providers' records. In all cases, providers accessing records are making an explicit or implicit commitment to use those records for legally permissible purposes. The sheer volume of data transmissions and the reliance by HIE participants on the privacy compliance infrastructure of their colleagues raises the risk that an organization will face privacy-related claims or investigations based on the conduct of other entities.

Convincing organizations to accept this risk usually requires the creation of mutual trust through the development and enforcement of stringent privacy standards that apply to all participants. It may also entail a contracting framework that imposes indemnification and insurance obligations on participants as well as the HIE.

* * * * *

State and regional HIEs are the building blocks of a national electronic health information network that at some point in the future is likely to connect health care organizations across the country. But before a national health data network can be come a reality, the above privacy issues, among others, will have to be resolved to the satisfaction of a divergent group of stakeholders. State and regional HIEs can serve as laboratories for resolving these issues, testing new ways to achieve consensus on the proper balance between patient privacy and effective health service delivery.

[11] .*See IMS Health v. Sorrell*, No. 10-79 (U.S Supreme Court, June 23, 2011).

[12] 45 C.F.R. § 164.514(a).

[13] 45 C.F.R. § 164.512(b).

[14] *See*, *e.g.*, N.C. General Statutes § 90-413.7(a)(3).

[15] 45 C.F.R. § 164.524(a)(3).