A Publication of the American Health Lawyers Association
Health Information & Technology Practice Group

Volume 15
Issue 1
March 2012

HIT News

This issue of HIT News *is sponsored by the*
Electronic Health Records Affinity Group

A Primer on Electronic Health Information Exchange Contracting Issues and Concepts

John R. Christiansen, Esquire
Christiansen IT Law
Seattle, WA

Contracting for electronic health information exchange (eHIE) can be frustrating. While eHIE seems simple in concept, and sometimes is in practice, it presents difficult technical and legal issues. As a result, deceptively simple concepts can sprout esoteric legal acronyms and opaque, hard-to-read contracts.

An in-depth analysis of eHIE contracting issues is well beyond this article's scope. Rather, this article flags some of the key issues eHIE contracts have to address, and reviews some key variations in eHIE network architecture and governance that may affect contracting. Understanding the issues eHIE presents should help illuminate some of the reasons for the network and governance variations, and make eHIE contract documentation somewhat easier to work with.

Making eHIE Networks Work

At first glance, eHIE seems as if it should be a simple, straight-forward importation of existing health information exchange processes into a new medium. Health information exchange goes on all the time, and has for a long time. Doctors and hospitals have been mailing and faxing medical records to each other since, well, the dawn of medical records and faxes. Providers share health information with public health agencies, both voluntarily and by legal mandate, and many more examples of HIE transactions are so common they are taken for granted.

The processes of HIE using traditional media are so familiar we usually do not even think about them. A practice using paper records, which refers a patient to a hospital, might fax over a copy of relevant portions of the medical record, and when a procedure is done, the hospital might copy and mail back relevant portions of its own paper records in return. It just seems to make sense that if both are using electronic medical records instead, all they would need to do is make electronic copies of the relevant records and transmit them to each other, so each can paste the other's copy into its own records. Nobody seems to think that parties to the former exchange using traditional media need a contract to govern the transaction, so why would they need one for the latter eHIE exchange?

Table of Contents

A Primer on Electronic Health Information Exchange Contracting Issues and Concepts
John Christiansen, Esq...1

Implementing EHRs: Strategies for Avoiding Disputes With EHR Vendors and Increasing Provider Leverage
Marcus Hewitt, Esq.
Antonia Peck, Esq....5

Reducing Risk in the Implementation of Electronic Record Systems: Practical Considerations and Benefits of a Risk Assessment
Frank Carsonie, Esq.
John DiMaggio..8

Editors' Notes
Patricia King, Esq.
Kevin Lyles, Esq.
Laird Pisto, Esq...12

Identifying, Managing, and Allocating EHR-Related Patient Safety Risks
Kathryn Heagerty, BSN, JD
Kevin Klauer, DO, EJD, FACEP
Debra Alligood White, Esq.................................13

"Enriched" EHRs: The Value of Integrating Payor Data and Associated Challenges
Matthew Haddad, Esq.
Angela Saverice-Rohan, Esq..............................16

AMERICAN
HEALTH LAWYERS
ASSOCIATION

"This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought."
—from a declaration of the American Bar Association

There are four problems that prevent application of traditional HIE concepts to eHIE, and make eHIE contracts prudent even though they are not legally required. The first problem is that unlike words or images on paper or film that are read by human eyes, a digital record is code that a receiving computer executes to create a duplicate record, which only then can be read by human eyes. This means the receiving computer needs to have the right software to read the code and create the record. It also means the duplication process can be subverted or corrupted, so that, for example, the sender is misidentified, record contents are altered, or the receiving computer is instructed to secretly send copies of the record to an identity thief in another country.

The second problem concerns the identification of specific records with specific data subjects. Different organizations often use different codes or algorithms to identify individuals, and the transmission of an incorrectly identified record would be a breach of confidentiality (though hopefully not a harmful one), and, if not caught, might lead to incorrect diagnostic, treatment, payment, or other decisions. In traditional HIE this problem is solved by manual review and reconciliation, a relatively time-consuming process that would interfere with genuinely efficient eHIE.

The third problem is that security standards for eHIE are immature. Traditional HIE entails physical (or fixed phone-line) movement from one place to another using processes governed by mature industry standards and practices that minimize the risk that records will be sent to, or intercepted by, unauthorized parties. In contrast, eHIE takes place in electronic networks linking many participants and not really designed for secure transactions, for which industry standards and practices are just emerging. Any computer that can connect to the network might be able to send or receive transactions, including transactions that are erroneous or fraudulent, in the absence of well-established standards and practices that could prevent them. At the same time, as the network expands, there are more possible locations for records, adding to the potential to miss necessary, available information.

The first three problems interact to create the fourth: lack of trust, on the part of both eHIE participants and the community served by the eHIE. Participants need to be able to trust that the potential for error and fraud is low enough, and standards and practices settled enough, that they are not exposed to: significant risk of harm to their systems caused by malicious code; harm to patients or the organization caused by incorrect or corrupted information; or legal liabilities if error or fraud causes an unauthorized disclosure of confidential information or harm to an individual or another party's systems or organization. Likewise, individuals whose sensitive personal information is being shared through eHIE need to be able to trust that the processes are technically sound and managed competently to avoid risks that their information will be stolen or otherwise come into the possession of parties who will use it for identity theft or other harm.

To make an eHIE network work, then, requires certain "rules of the road" that control at least the following issues:

- Form and content of transactions to ensure digital records that are sent can be accurately read on the receiving end;
- Safeguards against undetected alterations of transaction content;
- Safeguards against the transmission of malicious code in transactions;
- Common identifiers for individual data subjects, such as a master patient index (MPI);
- Systems for identification and authentication of participants (I&A), so that sending parties are assured they are sending to authorized receivers, and receiving parties are assured they are receiving from a trusted source;
- Safeguards against erroneous or fraudulent routing of transactions;
- A record locator service (RLS) or other mechanism for finding records; and
- Safeguards against viewing or use of content obtained by unauthorized parties by fraud or error.

The specific policies, processes, and technologies used to resolve these issues vary considerably, but they arise in the use of any eHIE network and all eHIE contracts need to address them somehow. This is the function of eHIE governance.

Any eHIE arrangement must be understood both at the network architecture level and the governance level.[1] Network architecture refers to the technology arrangements used to implement eHIE (the distribution and connection of software, servers, workstations, and other hardware through which transactions take place), while governance refers to the web of agreements and representations that govern the legal relationships among eHIE participants and their transactions. While there are no legal requirements or technical guidelines for integrating the two, governance must at least be consistent with network architecture. Governance that identifies relationships or establishes obligations or representations not consistent with the technical realities of the actual eHIE transactions will at least make it more difficult to solve inevitable problems and disputes, and at worst could cause an eHIE initiative to fail.

Understanding eHIE Architectures

From the architectural point of view, the building blocks of any eHIE include a digital data storage facility (repository), a participant with a computer who can request and obtain information from the repository, and a digital transmission connection between the two. Repositories can in principle be anything from an electronic health record in a workstation to multiple servers in a data center, or even distributed storage in a computing "cloud."

The building blocks can be combined in a number of ways, but three basic architectures can be identified.

- *Repository*—A "centralized repository" or "community health record system" is the most-centralized architecture, in which data from the various participating organizations is aggregated into a single repository for access by authorized users.
- *Federated*— Sometimes called "hub-and-spoke," "data warehouse-silo," or "federated repository" system, in this architecture different participating organizations store health information on their own and/or others' behalf in separate

repositories each organization maintains, and make it available to other participants upon request.

- *Pointer*—A "pointer" or "point-to-point" system is the least-centralized architecture, in which network HIE services (such as an MPI and/or RLS) allow authorized users to identify records stored by the various participants, so that they can directly request the information from the holder.

Network architecture has important implications for contracting. Repositories in particular are highly sensitive facilities and potential targets for malicious actors. The information they store is protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) and usually also subject to protection by state laws, is probably valuable for identity theft purposes, and may be embarrassing or harmful to individuals' reputations if disclosed. The more information a repository contains, the more valuable it is as a target.

I&A, MPI, and RLS systems also will contain legally protected, sensitive information that might be valuable for criminal activities. I&A requires registration of individual users, which generally entails collection and retention of their personal information, perhaps including Social Security numbers or other identifiers. The passwords or other identification tokens issued for I&A purposes may themselves be used to "spoof" a user's identity and gain unauthorized access to information and resources. MPI and RLS information may not include much beyond information identifying a specific individual as a patient of a specific organization, but that is still PHI subject to HIPAA. I&A, MPI, and RLS information also has to be protected against undetected alterations.

The variability of network architectures means the distribution of sensitive repositories and systems also is variable. In some arrangements—a fully outsourced community health record system, for example—the eHIE repository as well as I&A and MPI services might be housed in a centralized facility not owned by any of the participants. (An RLS would not be needed, because all records would be located in the repository.) In other arrangements, a number of hospitals and practices in a community might host their own repositories, but outsource I&A, MPI, and RLS services—or different participants might assume responsibility for common I&A, MPI, and RLS services.

This potential variability is the reason it is essential to understand the network architecture when contracting to establish or participate in eHIE. This becomes even more necessary when the additional complexities of governance are added to the mix.

eHIE Legal Relationships

Development of eHIE network architecture may often be easier than development of eHIE governance. In any given network, different entities may own a number of network components, and have varying rights to use or access the network. At the same time, most of the hardware and software on the network is vulnerable to unauthorized use for potentially harmful network access. All participants, as well as the party responsible for operating the network, therefore risk the loss of important data and critical processes if other parties fail to prevent unauthorized use or access. The decision whether to participate in eHIE therefore often depends on the extent to which network participants are exposed to both risks of loss and legal liabilities if their own systems or activities are compromised and used to cause losses to other participants. Because there are currently no laws specifically controlling eHIE obligations and liabilities, it is up to the participants to agree to their allocation. This is done through some form of contract, typically in the form of one-to-one or one-to-many forms of data sharing agreement, or bylaws for participation in a HIE organization such as a subnetwork organization (SNO), health information organization (HIO) including regional HIO (RHIO), or HIE (not to be confused with HIE as an activity).[2] There may or may not be important distinctions among these various types of entity; for most purposes:

> the most useful approach may be to consider that [eHIE] is an activity which takes place over electronic communications networks involving use of EHRs and related applications, organized by a state, private entity or consortium of entities, which includes those entities necessary to make the [eHIE] activity self-sustaining. The network may be operated by one or more entities, and may be called a RHIO, a RHIN, a SNO, a HIE initiative or organization, or something else; the parties may define their relationships by a 'web of contracts,' it may even be an informally organized coalition of entities using a public network such as the Internet. However the network is implemented, it is distinguished by the fact that it is used by entities for purposes of [eHIE.][3]

Whatever the eHIE governance arrangement is called, it is generally possible to categorize eHIE governance models along a spectrum from "open" to "closed:"[4]

- *Enterprise*—An enterprise HIO is typically operated by and principally for a single organization (one or more legally associated entities). This is a relatively "closed" system, typically available only to the enterprise and some of its trading partners. For example, Kaiser Permanente and the Mayo Clinic, both integrated health systems, each operate enterprise HIOs principally serving their own affiliates.[5]
- *Standard*—A "standard"[6] HIO is based on agreements among a group of entities in a given region or market that have identified business reasons for sharing information, typically because they serve common or overlapping populations. This is the "classic" RHIO model, though governance may be more or less formal. This is a more "open" model than the enterprise, and is often available on a limited geographic basis (e.g. local or regional), to a limited class of entities (e.g., providers but not plans). Examples of this model include Texas Mental Health Services and WellPoint's Individual Health Record system—both are operated by one organization but are intended for use for limited, defined purposes by the various providers that serve the same population.[7]
- *Utility*—Some HIEs may do little more than set up services providers (which might be participating healthcare organizations acting as services providers) to provide various technical

services allowing organizations to exchange information, with minimal restrictions or direction of transaction purposes and relatively "light" contract requirements. HealthBridge[8] and the OneHealthPort HIE[9] are both examples of utility HIEs.

From a contracting point of view, the important variation among these governance models is not only how open they are, but the "weight" of the governance, meaning the degree of freedom each leaves to participants in dealing with key transaction purpose and security issues. All network governance models need to provide for common I&A, MPI, and RLS solutions, or transactions will be too burdensome or unreliable. Transaction purpose and security issues, on the other hand, can either be dealt with by specific direction from the governing authority, or can be dealt with by participants at their reasonable discretion subject to liability for failure.

In the "heavy" governance model, eHIE participation requires conformance to centralized compliance requirements, while the light model generally limits direction to those areas specifically needed to protect network functioning. For example, under light governance, the eHIE administrative authority may need to require users to protect their passwords or other I&A tokens from compromise, to ensure transaction reliability, but probably would not specify the software participants use to protect against malicious software. However, eHIE contract provisions would make the participant liable for a failure to provide virus protection that allowed malicious software to infect another's system.

There does not seem to be a necessary relationship between governance models and governance weight, but it seems likely that the more open the model, the lighter the governance. An enterprise HIO has the ability, and from a risk management perspective probably the need, to manage compliance and exposures tightly by promulgating and enforcing specified policies and technologies. A standard or utility HIO, on the other hand, has to be able to attract participants to succeed, and lighter governance may be more attractive to most independent entities.

Conclusion

There is no single model for successful eHIE contracting—or, at least, no single model has emerged that seems likely to be the most successful. Variations in network architecture and governance openness and weight are essential in deciding what kind of contract provisions work, and how they may affect different organizations. This can only be determined by a case-by-case analysis and a sound understanding of the participants' goals in engaging in eHIE.

[1] This analysis is based on Christiansen, Apgar, and Melamed, *State and Federal Consent Laws Affecting Interstate Health Information Exchange* (National Governors Association 2011) at 10–12 (*NGA Report*). *See also* Rosati and Lamar, eds., *The Quest for Interoperable Health Records: A Guide to Legal Issues in Establishing Health Information Networks* (American Health Lawyers Association 2005) and Rosenbaum, Borzi, Repasch, Burke, and Benevelli, *Charting the Legal Environment of Health Information* (Robert Wood Johnson Foundation 2005).

[2] RHIO was a common term a few years ago, while SNO seems not to have caught on and HIE permits too much confusion. *See* Christiansen, *Legal Speed Bumps on the Road to Health Information Exchange*, 1 J. Health & Life Sci. 1, at 12–14 (Jan. 2008).

[3] *Id.* at 14.

[4] *See NGA Report, supra* note 1, at 11.

[5] *See id.* at 32-41.

[6] This term is not intended to suggest this is a legal standard or even that it is necessarily the norm, only that it appears to encompass the most common approach to HIE governance.

[7] *See* NGA Report, *supra* note 1, at 43-50.

[8] *Id.* at 28-30.

[9] *See* OneHealthPort HIE webpage *at* www.onehealthport.com/hieindex.php (visited Jan. 2, 2012).

Practice Groups Staff

Trinita Robinson
Vice President of Practice Groups
(202) 833-6943
trobinson@healthlawyers.org

Magdalena Wencel
Senior Manager of Practice Groups
(202) 833-0769
mwencel@healthlawyers.org

Denis Vidal
Practice Groups Administrator
(202) 833-0782
dvidal@healthlawyers.org

Crystal Taylor
Practice Groups Coordinator
(202) 833-0763
ctaylor@healthlawyers.org

Brian Davis
Practice Groups Editorial Coordinator
(202) 833-6951
bdavis@healthlawyers.org

Ramon Ramirez
Practice Groups Coordinator
(202) 833-0761
rramirez@healthlawyers.org

Tazeen Dhanani
Practice Groups Web Assistant
(202) 833-6940
tdhanani@healthlawyers.org

Graphic Design Staff

Mary Boutsikaris
Creative Director
(202) 833-0764
mboutsik@healthlawyers.org

Ana Tobin
Graphics Assistant
(202) 833-0781
atobin@healthlawyers.org