Liability Coverage for Regional Health Information Organizations

Lessons from the AHRQ-Funded State and Regional Demonstration Projects in Health Information Technology and Other Community Efforts

Prepared for:
Agency for Healthcare Research and Quality
U.S. Department of Health and Human Services
540 Gaither Road
Rockville, MD 20850
www.ahrq.gov

Prepared by:

Prashila Dullabh, M.D.
Maria Molfino, B.A.
Robert S. Rudin, S.M.

National Opinion Research Center
AHRQ National Resource Center for Health Information Technology

AHRQ Publication No. 09-0071-EF
June 2009

Suggested Citation:
Dullabh P, Molfino M, Rudin RS. Liability Coverage for Regional Health Information Organizations: Lessons from the AHRQ-Funded State and Regional Demonstration Projects in Health Information Technology and Other Community Efforts. Prepared by the National Opinion Research Center, AHRQ National Resource Center for Health Information Technology. AHRQ Publication No. 09-0071-EF. Rockville, Maryland: Agency for Healthcare Research and Quality. June 2009.

Acknowledgments

We are grateful to the participating State and Regional Demonstration Projects, other Health Information Organizations, and key people who provided us with the information to develop this report.

This document was prepared by staff of the Agency for Healthcare Research and Quality (AHRQ) National Resource Center for Health Information Technology, under AHRQ Contract Number 290-04-0016.

FOREWORD

The National Opinion Research Center (NORC) at the University of Chicago is pleased to present this report entitled *Liability Coverage for Regional Health Information Organizations: Lessons from the AHRQ-Funded State and Regional Demonstration Projects in Health Information Technology and Other Community Efforts*. The Agency for Healthcare Research and Quality (AHRQ) awarded six States 5-year contracts under the State and Regional Demonstrations in Health Information Technology (Health IT) request for proposals. As Health Information Organizations (HIOs),[1] the State and regional demonstrations (SRDs) support State- and regional-level health information exchange (HIE). HIOs are multistakeholder organizations that enable secure HIE, which offers tremendous potential to improve health care quality, reduce medical errors, and lower costs. Contracts for the SRDs began in October 2004 for five States: Colorado, Indiana, Rhode Island, Tennessee, and Utah. The State of Delaware started its contract in October 2005. The six States are currently developing a variety of approaches to HIE, with different technical, business, and governance models.

The AHRQ Health IT portfolio consists of various grants and contracts that have planned, implemented, and evaluated the impact of various information technologies on the quality, safety, and efficiency of health care delivery. Between 2004 and 2006, the AHRQ awarded over $166 million in funding as part of the Health IT portfolio, an estimated $30 million of which was awarded to the SRDs. In 2007 and 2008, AHRQ awarded another 75 Health IT grants in ambulatory safety and quality, totaling approximately $85 million, in addition to contracts related to various specific health IT topics such as e-prescribing and clinical decision support. Additionally, the AHRQ Health IT portfolio includes the National Resource Center for Health IT (NRC), created to support the many projects funded by AHRQ and others in adopting and evaluating health IT and HIE efforts. The NRC has established an infrastructure for collecting, analyzing, and disseminating best practices and lessons learned from AHRQ's portfolio of Health IT projects.

The six SRDs, and the two other community efforts reviewed in this report, have each developed an HIO. To protect themselves from liability, HIOs must understand the risks involved with HIE and determine how these risks are shared among their participating entities. HIOs and their participating entities are currently navigating this new and immature area of HIE liability. The primary purpose of this report is to share lessons learned from the field on the key considerations, issues, and challenges associated with liability insurance for HIE.

[1] As part of its work under the sponsorship of the Office of the National Coordinator for Health IT (ONC), the National Alliance for Health Information Technology (NAHIT) provides definitions for many of the key concepts related to health information exchange (HIE), for example: Health information exchange is "the electronic movement of health-related information among organizations according to nationally recognized standards." And: A health information organization (HIO) is "an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards." The types of data involved in HIE may include demographic data and patient medical history, data on medical conditions, diagnoses, procedures, allergies, and therapies collected at the point of care and data collected and used for administrative purposes including claims.

TABLE OF CONTENTS

BACKGROUND

Regional health information organizations (RHIOs)[2] bring together health care stakeholders within a defined geographic area, and govern health information exchange (HIE) among these stakeholders for the purpose of improving health care in that community. RHIO stakeholders may include hospitals, primary care physicians, specialty physicians, laboratories, radiology centers, and health plans—all of which consolidate efforts to facilitate HIE. The eHealth Initiative (eHI) has developed a framework to assess and track the growth of RHIOs and has identified seven stages of development. There are four pre-operational stages: recognizing the need for HIE (Stage 1), getting organized (Stage 2), transferring vision (Stage 3), and getting implementation underway (Stage 4). In addition, there are three fully operational stages of development: transferring data among stakeholders (Stage 5), transferring data based on a sustainable business plan (Stage 6), and finally, demonstrating expansion of the organization (Stage 7).[3]

The eHealth Initiative's *Fourth Annual Survey of Health Information Exchange at the State, Regional, and Community Levels* noted that, between 2006 and 2007, 30 RHIOs had advanced from at least one of these stages of development to the next,[4] *The Fifth Annual Survey of Health Information Exchange at the State and Local Levels* revealed that in 2008, 42 of 130 HIE initiatives self-identified as fully operational (Stages 5 - 7), representing a 31-percent increase since 2007.[5] These surveys suggest that RHIOs are moving evenly through various stages of development and that the number of fully operational RHIOs will continue to grow in the future.

---

[2] NAHIT defines a regional health information organization (RHIO) as "an HIO that brings together health care stakeholders within a defined geographic area and governs HIE among them for the purpose of improving health and care in that community."

[3] eHealth Initiative, (Washington, DC: 2008). http://www.ehealthinitiative.org/HIESurvey/2008StateOfTheField.mspx. Accessed on May 26, 2009.

[4] eHealth Initiative, eHealth Initiative Fourth Annual Survey of Health Information Exchange at the State, Regional, and Community Levels (Washington, DC: 2008). http://www.ehealthinitiative.org/HIESurvey/2007Survey.mspx. Accessed on May 26, 2009.

[5] eHealth Initiative, eHealth Initiative Fifth Annual Survey of Health Information Exchange at the State, Regional, and Community Levels (Washington, DC: 2008). http://www.ehealthinitiative.org/HIESurvey/2008StateOfTheField.mspx. Accessed on May 26, 2009.

As the field of HIE continues to expand, questions surrounding liability have become a central concern to RHIOs and their partners. Liability is the legal responsibility for one's acts or omissions.[6] Failure of an entity—or person within that entity—to meet that responsibility leaves the entity open to a lawsuit for resulting damages. In the context of this report, we focus on civil liability, which is the potential responsibility for payment or damages or other court-enforced ruling in a lawsuit.[7] Therefore, an entity is liable when it is "legally responsible for paying for damage or loss incurred."[8] Generally, liability is applicable under several circumstances; RHIOs, however, are primarily concerned with liability in the context of negligence. Negligence is defined as "failure to give proper care to something, especially a duty or responsibility, with the result that a person or property is harmed."[9] The injured party must prove that the RHIO did not take reasonable and appropriate actions, and thus caused the injured party harm.

The Health Insurance Portability and Accountability Act (HIPAA) is a Federal law that provides privacy and security guidelines on reasonable and appropriate actions regarding the storage and exchange of protected health information (PHI). PHI is defined as information that relates to the physical or mental health of an individual, the provision of health care to an individual, or the payment for provision of health care to an individual, created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.[10] The HIPAA regulation therefore covers health plans, health care providers, and health care clearinghouses, all commonly referred to as HIPAA "covered entities," but does not directly apply to RHIOs. As organizations performing functions involving PHI on behalf of a HIPAA-covered entity, RHIOs are bound by the business associate agreement (BAA) that HIPAA requires for such relationships. The American Recovery and Reinvestment Act (ARRA) of 2009[11]—

---

[6] LAW.com /Dictionary, Accessed on May 26, 2009.

[7] LAW.com/ Dictionary

[8] In Dictionary of Law. London: A&C Black. http://dictionary.law.com/default2.asp?selected=1314&bold=||||Accessed on December 05, 2008.

[9]Ibid.

[10] CMS. The HIPPA Law and Related Information. http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf Accessed on May 26, 2009.

[11] Discussions of HITECH—sections of ARRA relating to HIT and referred to as the "HITECH Act"—throughout this paper draw on the following sources: Healthcare Information and Management Systems

the recently passed stimulus package providing over $20 billion in funding for health IT—suggests that these HIPAA regulations will be extended to business associates of covered entities such as RHIOs. The statute implies that RHIOs will ultimately (1) be required to comply with the administrative, physical, and technical safeguards of the HIPAA security rule provisions; (2) be required to adhere to the terms of their BAA on the use and disclosure of PHI; and (3) be subject to the same civil and criminal penalties as covered entities in the event that they violate these requirements.[12] The implications for RHIOs of this expected change remain unknown; in particular, the potential impact on their liability insurance will need to be examined in the near future.

As hosts and conveyers of the electronic exchange of clinical information, RHIOs must manage against threats such as data theft, accidental disclosure of patient information, data errors and omissions, and technology failures. To protect themselves from negligent actions, RHIOs around the country have considered the purchase of appropriate liability insurance. RHIOs must make several decisions related to liability. Listed below are the key issues identified by RHIOs and representatives in the area of liability insurance for HIE.

- How do RHIOs distribute liability among partners?
- Which partnering entities currently take on liabilities? What are the liability concerns of RHIO partners?
- What levels of liability coverage are appropriate? What factors affect these levels of coverage?
- How do RHIOs find and manage brokers and underwriters[13]?
- What are the impacts of law and government on a RHIO's liability?

Society, "HIMSS Summary of Key Health Information Technology Provisions," February 2009; Redhead, C. Stephen (2009). The Health Information Technology for Economic and Clinical Health (HITECH) Act. Washington, DC: Congressional Research Service; and Mannatt, Phelps & Phillips, LLP, "Health IT Provisions in Final Federal Stimulus Package," February 2009.

[12] Ibid.

[13] For the purposes of this report, an underwriter is a person or company that underwrites and issues the insurance policy. An insurance broker aims to find the best policy by comparison shopping and negotiates premiums with the insurance company (i.e. the insurance carrier) in order to sell the best policy to his/her client.

Because regional exchange of clinical information is relatively new, the insurance industry has not yet established standard approaches to addressing a RHIO's potential liability. Discussions with field representatives suggest that few underwriters offer applicable policies to address this issue. A closer examination of liability insurance issues in the field may therefore help reduce duplicative efforts and minimize the resources RHIOs will need to invest to answer the questions outlined above. This report will share findings from the field on how eight RHIOs, including the six AHRQ-funded SRD projects, have navigated various issues and challenges associated with liability insurance for HIE. This report also includes recommendations from HIO representatives, lawyers, insurance agents, and other industry representatives regarding the future handling of select liability problems. The intended audience of this report includes the SRDs, the broader RHIO and HIE industry, and Federal agencies involved in HIE efforts including the Office of the National Coordinator for HIT (ONC), the Health Resources and Services Administration (HRSA), and the Centers for Medicare & Medicaid Services (CMS).

DISCUSSIONS WITH RHIO LEADERS AND OTHER REPRESENTATIVES

The information in this report was gathered through an environmental scan of published and unpublished materials on liability insurance and HIE written in the last 5 years. The environmental scan, however, revealed that little to no research had been produced on these topics, thus prompting the National Resource Center (NRC) for Health Information Technology to discuss the current liability insurance landscape with various RHIO leaders and other representatives. The NRC held discussions with the six SRD projects—the Colorado Regional Health Information Organization (CORHIO), the Delaware Health Information Network (DHIN), the Indiana Network for Patient Care (INPC), the MidSouth eHealth Alliance (MSeHA), the Rhode Island Quality Institute (RIQI), and the Utah Health Information Network (UHIN)—and two other well-established RHIOs in the industry: the Taconic Health Information Network Community (THINC) in Hudson Valley, New York; and HealthBridge in Cincinnati, Ohio.

In addition to this core set of RHIO leaders, the NRC then used a classic "snowballing technique" to identify additional resources and/or respondents with experience in this area and related areas. The NRC asked RHIO respondents to identify other individuals who could inform the development of the report; respondents referred the NRC to attorneys, insurance agents, and other fellow RHIO representatives for discussions. Appendix A lists the original respondents and these additional individuals. Appendix B provides sample questions used to guide discussions with respondents. However, the actual questions asked during each discussion were tailored to reflect the unique profile of each RHIO as well as the nature of the respondent's expertise.

The remainder of this report explores the important aspects of today's liability landscape and specifically discusses the approaches taken by a subset of RHIOs to distributing liability among their partners and to obtaining insurance coverage. In addition, we discuss how government involvement in RHIO creation can potentially alter the liability landscape for the RHIO and its partners. Specifically, we discuss the experiences of the Delaware Health Information Network, which was created with strong government involvement. We then summarize key lessons across the RHIOs on

how to plan for and manage liability in order to further inform future RHIO liability insurance efforts.

RHIO Liability Landscape

Through our review of the available literature and discussions with various respondents for this report, we found what appears to be a well-accepted expectation that RHIOs will purchase liability insurance. Although every RHIO is unique, RHIOs often face similar challenges in negotiating liability among partners and purchasing liability insurance. All RHIOs, for example, rely heavily on the participation of community stakeholders to advance their activities. RHIO participants may include ambulatory providers, laboratories (local, national, or reference), hospitals, public health agencies, healthcare payors, information technology (IT) vendors, and others.[14] The RHIO and its participants are involved in the exchange of protected health information (PHI) through various complex governance and connectivity arrangements. In the event of injury or harm to a third party as the result of negligence, the RHIO and/or its various participants may be held liable. Because exchange of data does not occur in a vacuum, RHIO stakeholders (including both data providers and data users) may want to define in advance how liability resulting from future events will be apportioned among themselves and the RHIO. Given the hierarchical operational structure of RHIOs, vicarious liability[15] is a concern for all stakeholders—that is, a RHIO may be found liable for the harmful actions of its participants (or vice versa). Negligence resulting in the harm or injury of a party may occur as the consequence of a wide range of actions or inactions, which include inappropriate disclosure of patient data (due to theft or accident), errors and omissions in data entry, failure of data users to utilize available data, and technology malfunction resulting in erroneous data.[16] Negligence may also arise from mismanagement; for example, hiring unskilled or untrained staff, failing to supervise staff appropriately, and neglecting to implement proper policies. These actions and inactions may result in injury or harm, and damages could result either from a violation of patient privacy or a negative health outcome. In addition to BAAs, RHIOs also typically develop and enter into master data sharing agreements (MDSAs) with their various partners. MDSAs

[14] Note that these stakeholder groups can be both data sources and data users.

[15] Vicarious liability; sometimes called "imputed liability," means the attachment of responsibility to a person for harm or damages caused by another person in either a negligence lawsuit or a criminal prosecution. Thus, an employer of an employee who injures someone through negligence while in the scope of employment (doing work for the employer) is vicariously liable for damages to the injured person (http://dictionary.law.com/Dictionary).

[16] Note that liability insurance does not cover actions of malicious or criminal intent.

commonly indicate the criteria for data provision, data access, privacy, and confidentiality to ensure data security and the secondary/research uses of data. There is a tremendous variability in the MDSA terms used by RHIOs to address the specific liability issues and concerns in their respective arrangements. The practice of addressing such concerns in MDSAs is not uncommon, especially in cases where some partners have legal immunity and others do not. In addition to this core set of agreements, some RHIOs may decide to address liability issues with a specific data provider in a separate business agreement.

The distribution of liability is typically a collective decision and can be a lengthy process requiring considerable negotiation to ensure the agreement of all parties in the sharing of liability. Large and reputable IT vendors, for example, often refuse to accept liability from a small RHIO. Liability insurance relevant to RHIOs and their partners include the following types.[17]

- Directors and Officers insurance (D&O): provides financial protection for the directors and officers of one's organization in the event they are sued in conjunction with the performance of their duties as they relate to the organization.[18]
- Errors and Omissions insurance (E&O) and Cyberliability: protects the organization from claims if the client holds it responsible for errors, or the failure of the organization to perform as promised in the contract. This coverage is concerned with performance failures and negligence with respect to products and services.[19]
- Product Liability (for IT vendors): indemnifies a manufacturer, supplier, or retailer from liability to a purchaser or user caused by a foreseeable defect in the product.
- Malpractice insurance (for physicians): indemnifies a physician for negligence (conduct that falls below the customary standard of care) related to professional medical decisions.

There is great uncertainty regarding who would be subject to a lawsuit and under what circumstances. For example, what would happen if a RHIO received incorrect information from a participating entity which resulted in an adverse patient health outcome? RHIOs have attempted to

[17] Other kinds of liability may be obtained by RHIOs but are not relevant to this report (e.g., automotive insurance).

[18] Insure Pro. Professional Liability Coverage: Directors and Officers Insurance Explained. http://www.insurepro.net/html/directors_and_officers_explained.asp. Accessed on May 20, 2009.

[19] Ibid.

address these hypothetical scenarios through MDSAs, BAAs, and other contracts with their partners. The absence of case history of lawsuits regarding liability for RHIOs, however, has continued to generate uncertainty with respect to the liability that could be incurred by RHIOs. This uncertainty has lead to: (1) the perception that all stakeholders could be named in the case of a lawsuit, and (2) challenges in setting and negotiating appropriate levels of coverage and premiums and coordinating policies between different entities.

Attempts to estimate the level of risk is complicated by other factors. Insurance companies traditionally calculate coverage offered by examining the revenue of the organization, an approach not applicable to RHIOs, which rarely have assets, are generally organized as non-profits, and rely heavily on grants. A more sensible approach for calculating risk may be to examine a RHIO's functionality and technical architecture. For example, the degree of risk associated with clinical results delivery functionality will likely differ with the level of risk associated with record query functionality. Similarly, a federated technical architecture may be associated with a different level of risk than a centralized technical architecture. However, there are currently no standard practices or methodologies to assess risk based on functionalities or technical architecture, and risk assessments vary by RHIO.

Our discussions with RHIO leaders and other representatives suggest that in this complex and fledgling environment, few underwriters offer liability policies for RHIOs. Those who do offer policies may still not fully understand the operation and accompanying risks (or lack thereof) of a RHIO. Due to this lack of understanding, underwriters may charge more than is necessary. Other factors that may contribute to inflated rates are RHIOs' lack of track records and assets, and the uncertainty of the size of damages that could result from a lawsuit. Brokers and underwriters are becoming increasingly educated about RHIOs, but existing policies have yet to be tested in court. However, in some cases, a RHIO's partners have concerns that stem from lawsuits in the identity theft arena.

Our discussions also addressed the ways that Federal and State laws and regulations affect liability issues for RHIOs. In particular, the DHIN avoided some of the difficulties related to liability by seeking protection through its State government. Other RHIO representatives, however, expressed the concern that certain State laws may create additional liability for the RHIO.

DISTRIBUTION OF LIABILITY

The issue of liability is of central concern to RHIOs and their partners. Before seeking liability coverage, RHIOs must understand and establish the distribution of liability among themselves and their many partners. Liability distribution requires significant business negotiation with all participating entities. Negotiations are often fraught with challenges because participating entities are reluctant to take on more liability than absolutely necessary.

In order to deal with liability, RHIOs establish business contracts, often in the form of MDSAs and BAAs, with their various partners that outline the level of liability coverage partners must carry. A RHIO may therefore contractually require its partners to carry a specified level of professional and general liability insurance as a condition for participation in data exchange. Some RHIOs, however, may only require their partners to carry what they believe is "reasonable and necessary." In some cases, a RHIO may require its partnering organizations to maintain insurance for a minimum period of time after leaving a RHIO. These business contracts may include indemnification clauses[20] that further delineate whether the partner or the RHIO would be held liable for damages in the occurrence of a lawsuit. Indemnification clauses specify who will pay penalties and who will be exempted from incurred penalties or liabilities. These clauses are added to business contracts with the assumption that the indemnifying partner has acquired enough liability coverage to pay for any potential damages or claims that may result from the negligent actions of the indemnified partner. For CORHIO, two of its four original participants are hospitals which are sufficiently related to State government that they benefit from sovereign immunity and may be prohibited by the State constitution from contractually assuming indemnification obligations. To address these market conditions, CORHIO has added special provisions to its MDSA which acknowledge the special characteristics of hospitals which are instrumentalities of the government.

Data Ownership: Key Factor in the Distribution of Liability

Discussions with RHIO leaders and other representatives suggest that the level of data ownership and management assumed by the RHIO and its partners primarily affects the distribution of liability. In general, the more authority the RHIO possesses in terms of ownership and management of data, the more liability coverage it will need to take on. For example, HealthBridge has a federated

[20] As an example, the RHIO may agree to indemnify and "hold harmless" the partnering organization (or vice versa) against any and all liability, claims, suits, losses, costs and legal fees caused by, arising out of, or resulting from any negligent act or omission of the partner in the performance and/or failure to perform within the contractual agreement including the negligent acts or omission of any partner or any direct or indirect employees of the partner.

model[21] but owns and operates a data center.[22] Consequently, all contracts with HealthBridge partners include indemnification clauses from all HealthBridge-related errors and omissions and for non-commercial quality problems such as inappropriate accessing of PHI. In this case, HealthBridge is obligated to take reasonable measures to safeguard data and is liable even when it does take those measures.

Like HealthBridge, most RHIOs in this report employed variations of a federated model, which means that each of their partners owns and stores the data separately. As a result, the RHIO often requires their partners to carry an amount of coverage and hold responsibility for the accuracy and completeness of the data they provide. The amount of this coverage, however, varies. There may also be State laws that specify what liability the partners of a RHIO should assume. For example, New York State law requires the partners (hospitals, commercial laboratories, and ambulatory physicians) of the THINC (a centrally managed federated model) to take on a significant amount of liability and to carry general liability insurance.

In cases where the RHIO largely serves the role of a 'switch' to route information, the liability assumed by partners may be higher. For example, the UHIN, which has set up a "post office" model where messages pass through the UHIN's hub but no data is centrally stored,[23] that all RHIO partners carry liability insurance. In other cases, the RHIO may not specify a fixed or minimum amount of coverage to be carried by partners. In the case of the MSeHA, which has a centrally managed federated architecture in which each data participant owns its data, all partnering organizations are required to carry a level of coverage that they believe is reasonable. Similarly, the INPC's approach is to affirm that each partner owns its data and is accordingly responsible for the amount of coverage it chooses to take on.

---

[21]In a federated model, data are stored on systems owned by the exchange participant. The most common form of this model includes a host at a central location. Data from exchange participants remain segregated, but are centrally managed by the governing entity which ensures a more uniform approach to the management and technical infrastructure. The lower risk of compromising data often encourages initial stakeholder buy-in.

[22] Public Governance Models for a Sustainable Health Information Exchange Industry, Report for the State Alliance for E-Health. http://www.nga.org/Files/pdf/0902EHEALTHHIEREPORT.PDF

[23] AHRQ. State and Regional Demonstration Projects: the UHIN. http://healthit.ahrq.gov/portal/server.pt?open=514&objID=5562&mode=2&holderDisplayURL=http://prodportallb.ahrq.gov:7087/publishedcontent/publish/communities/a_e/ahrq_funded_projects/srd_projects/projects/utah.html . Accessed on May 20, 2009.

On the other end of the spectrum, the DHIN, which was created as a State entity with sovereign immunity,[24] does not require any of its partners to have liability insurance (see *Impact of Government and Laws).* In some cases, the RHIO may have key partners that are government entities—such as public hospitals—that are either immune or have a limit to their liability. In the case of the MSeHA, some of the public hospitals in Tennessee fall under the Tennessee Claims Commission Act and are subject to limits of $1,000,000 per occurrence (i.e. total amount collective claimants can receive) with a maximum of $300,000 per claimant.

Liability Concerns of RHIO Participants

During discussions, respondents mentioned the various liability concerns of a RHIO's partners. Data sources, for example, are concerned with their liability in relation to the accuracy and completeness of the data they commit to the RHIO. RHIOs such as Healthbridge, the INPC, and the MSeHA contractually hold data sources liable for the accuracy and completeness of their data because these data sources essentially "own" the data. Although the DHIN does not require its partners to have any liability insurance, under the DHIN statute, data sources can be held responsible if they do not follow the rules and regulations for inputting and using the data as specified in contracts and MDSAs. In addition, RHIOs typically hold the data sources and users liable for any breach or disclosure that results from that stakeholder's errors. One legal expert, however, opines that contracts may tend to be vague about these kinds of breaches and disclosures.

Many respondents also mentioned the concept of "deep pockets." Given that many RHIOs have limited assets, generate little (if any) revenue, and are still largely dependent on grants, partners are concerned that they may be held accountable in a lawsuit, as trial lawyers will seek the participant with the "deepest pockets," that is, the most financial resources. Although this has not been a direct barrier to participation in a RHIO, various partners, especially those who are more financially viable such as health insurers and large hospitals, have voiced this as a central concern. Some partners, as in the case of CORHIO, have requested legal immunity for participating in the RHIO. These concerns are commonly addressed in the RHIO's various individualized business contracts with such partners.

[24] Sovereign immunity is a legal doctrine precluding the institution of a suit against the sovereign (in this case, the state government) without its consent. Therefore, the sovereign or State cannot commit a legal wrong and is immune from civil suit or criminal prosecution. (http://en.wikipedia.org/wiki/Sovereign_Immunity. Accessed on May 26, 2009.)

Partners are also concerned that their participation in the electronic flow of PHI will increase their liability, compared with the liability they bear in virtue of their participation in the paper world. For example, physicians may worry that, because data is available electronically, they will be required to use that data to a greater degree to inform their clinical practice than is currently expected by the standards and regulations of the paper world. Given that Web portals and electronic health records (EHRs) aggregate data, some providers are concerned that they will bear an increased responsibility to seek and review more readily available patient data. There are no widely recognized standards for reasonable physician behavior in seeking or reviewing electronically available data, or for the extent to which that data should inform his/her clinical decisions. A recent study, however, found that physicians with EHRs appear less likely to pay malpractice claims than physicians without EHRs, although this difference was not statistically significant after controlling for confounding variables (sex, race, year of medical school graduation, specialty, practice size, etc.)[25] Further research in this area is needed before the implications of a physician's participation in HIE on malpractice insurance can be fully understood.

RHIO partners may also be concerned that their participation in the electronic flow of PHI will increase their potential liability through the availability of electronic audit logs or access logs. Some RHIOs have recently been compelled via subpoena to provide information for malpractice lawsuits involving their partners. Regardless of who owns the electronic audit logs—ownership depends on the RHIO's technical architecture[26]—it is common practice for the custodian of the data to be the recipient of the subpoena, and in such cases the requested records would need to be produced and made available to the appropriate lawyers. One RHIO was subpoenaed for access log records and other details of information exchange as part of a malpractice lawsuit involving one of its partnering organizations. This RHIO reported that if such subpoenas continue, exchange partners, which include other hospitals, ambulatory providers, and physicians, will be concerned that participating in HIE could increase their liability.

[25] Virapongse A, Bates D, Ping S, et al. Electronic health records and malpractice claims in office practice. Arch Intern Med 2008;168(21):2362-7.

[26] In a federated model, the data sources often own the data and audit logs and would therefore be required to answer to the subpoena.

Extending Liability to IT Vendors

Information technology (IT) vendors also take on liability through business contracts with the RHIO. IT vendors might provide software, integration services, and operational services for the RHIO. All the RHIOs in this report tried to make their IT vendors take on liability, and most required them to have a certain amount of liability insurance. The level of coverage depended on the services provided by the vendors and the kinds of data the HIO stored or exchanged, i.e., whether clinical or administrative. Another factor that strongly influenced the liability assigned to IT vendors was the negotiating power of the RHIO. The type of coverage in their liability insurance that the IT vendors were asked to carry varied from general liability to more specific coverage related to hardware and software.

In general, all IT vendors were asked by their RHIOs to have a range of total liability coverage between $1 million and $3 million. The range differed depending on the services and software provided by the vendor. Although HealthBridge performs all the technical operations for the RHIO, it still requires all IT vendors to have $3 million as total liability coverage. In the case of the THINC, all IT services and IT infrastructure are the responsibility of its operational service provider MedAllies, and this is specified in the THINC/MedAllies contract. CORHIO, which employs a federated model and does not store any data centrally, has outsourced its responsibilities, and commensurate liabilities, to several IT vendors. CORHIO reported having varying degrees of success in its early efforts to negotiate insurance coverage requirements (less problematic) and indemnification requirements (more problematic), depending on the functions outsourced and the market presence of the vendor. CORHIO also reported that, now that it is operational and the Health IT market has begun to mature, it expects an improvement in indemnification coverage as its early contracts come up for renewal or replacement. In the case of the DHIN, all IT vendors are required to have certain amounts of liability insurance. Specifically, the DHIN requires their IT vendors to carry comprehensive total general liability coverage ranging between $1 million and $3 million, as well as one of the following types of insurance: medical/professional liability, errors and omissions, or product liability. The MSeHA is in a unique situation because at the time of the RHIO's formation Vanderbilt University was its IT vendor. The MSeHA was assessed at a lower risk because it had the structural and technical backing of the University; e.g., security infrastructure and firewalls. The MSeHA is currently transitioning to a new IT vendor, Informatics Corporation of America (ICA), and when this change takes place, both MSeHA's and ICA's liability insurance may

increase because ICA does not have the same reputation and credentials as Vanderbilt University. Lastly, the UHIN requires all IT vendors to carry total liability coverage of $2 million. The current rate applies only to administrative data exchange but is likely to increase when the clinical data exchange is added.

As the RHIO market matures and the range of services expand, there will be an increased need to ensure that all parties involved carry appropriate liability insurance. Many challenges remain, however, including the difficulties of negotiation of liability distribution, the lack of standardized liability distribution practices across RHIOs, the reluctance of the RHIO's partners to take on liability, as well as their various reservations with regards to how their liability will be affected when participating in HIE.

Liability Coverage and Premiums

Obtaining liability coverage is a burdensome process for many RHIOs. Some acquire a policy during an initial planning phase, while others wait until the RHIO is almost operational. A RHIO, on average, can spend from six to twelve months putting a liability insurance policy into place. For some RHIOs, DHIN for example, liability is central to how the organization is established. However, most consider obtaining liability coverage one of many necessary processes.

The RHIOs in this report used various processes to locate underwriters. Many used referrals from personal connections to find underwriters with some relevant experience, but some, such as the MSeHA and HealthBridge, went through a more thorough selection process. Locating underwriters has been challenging; a few years ago, one RHIO had only one choice for an underwriter, a situation that gave the RHIO limited negotiating power. Underwriters mentioned by respondents include ACE Professional Risk, Axis Surplus Insurance Co, Beazley, Chubb, Darwin, Great American Insurance Group, Hiscox, and Safeco. In terms of insurance brokers, the COHRIO relied heavily on their agent from Aon Corporation during most phases of the effort to obtain coverage and negotiate premiums. Similarly, HealthBridge hired a local agent[27] to find its underwriter. This agent conducted a lengthy nationwide search for a HIPAA-related insurance policy, because most general liability companies do not commonly have this coverage. It was only about two years ago, however, that HealthBridge found a policy specifically related to HIPAA disclosure (covering inappropriate disclosure of electronic data) with an affordable premium.

[27] Eppa Rixey from the Rixey Berry Agency in Cincinnati, Ohio.

Coverage

In addition to finding and educating an underwriter, the RHIO must determine level and types of coverage. Central to determining coverage is the potential level of damage and risk involved. Given the relative newness of this area for underwriters and insurers, there are no standard approaches to assessing the level of risk for a RHIO. To further confound matters, underwriters and insurers are likely to insure an entity based on the assets that it possesses and the revenue it generates. Given that there are few examples of RHIOs that possess assets and generate revenue, and that long term sustainability is one of the major issues of the HIE industry,[28] some of the organizations reviewed for this report indicated that RHIOs and their participating entities often have overlapping liability coverage to guard against the uncertainty of the level of risk and of the interpretation of the laws.

Table 1 summarizes the kinds of coverage acquired by the various RHIOs, the level of coverage obtained, and what is covered for RHIOs. The RHIOs profiled for this report, with the exception of the DHIN, all acquired Directors and Officers (D&O) insurance and Errors and Omissions (E&O) insurance. Among all the RHIOs interviewed, total D&O coverage generally ranges from $1 to $3 million and provides protections to the RHIO management and board of directors. Total E&O coverage ranges from $1 to $3 million and generally covers data theft, data mismanagement, problems with data generation, and data misuse. The UHIN, in addition to D&O and E&O, acquired an Ultra Office Policy for employment practices liability insurance with a total liability coverage of $2 million. The RHIO employees are covered under this policy. Few of the RHIOs studied for this report provide direct employee insurance. In some cases, the RHIO's employees are protected by state law, as is the case with the THINC, or else the RHIO subcontracts or outsources its staff, in which case the subcontractor is responsible for employee insurance.

TABLE 1. TYPES OF LIABILITY POLICIES BY RHIO

Table 1 describes the coverage types acquired by each RHIO and what is covered by these coverage types

NAME OF RHIO	COVERAGE TYPES	WHAT IS COVERED?
CORHIO *	• Directors & Officers (D&O): $1 million • Technology Errors & Omissions (E&O)	• D&O (executive protection) • Technical systems, software, data (e.g. data

[28] eHealth Initiative, eHealth Initiative Fifth Annual Survey of Health Information Exchange at the State, Regional, and Community Levels (Washington, DC: 2008). http://www.ehealthinitiative.org/HIESurvey/2008StateOfTheField.mspx. Accessed on May 26, 2009.

	(professional liability): $5 million • General Liability : $1 million (per occurrence) / $2 million (total)	breach) • Damage caused by CORHIO (business operations, fire, personal injury, etc.)
HealthBridge	▪ D&O: $3 million ▪ E&O: $3 million	• E&O covers theft and mismanagement. Current policy covers inappropriate disclosure of electronic data.
INPC*	▪ D&O: $1 million ▪ E&O: $1 million ▪ General Liability: $1 million (per occurrence) / $2 million(total) ▪ Umbrella Liability - $1million minimum ($5 million when dealing with state work)	▪ E&O covers technology exposure, errors and omissions, technology theft (internal and external), violating HIPAA, emergency response for mis-transferred data, and technology business interruption.
MSeHA*	▪ D&O: $2 million ▪ E&O: $1 million (per occurrence) / $3 million (total)	▪ E&O covers media and technology, data theft, data mismanagement, data generation and data misuse. ▪ MSeHA employees are subcontracted through Bioworks, who provides insurance for them.
RIQI*	▪ D& O: $ 1million ▪ E&O†: $1 million (per occurrence) / $2 million (total)	▪ D&O provides financial protection for the directors and officers in the performance of their duties as they relate to the organization.
THINC	▪ D&O: $1 million ▪ E&O: $3 million	▪ E&O covers theft, misuse and mismanagement. ▪ New York State gives employees of non-profit entities protection for employee liability, so THINC employees do not bear any liability.
UHIN*	▪ D&O: $1million ▪ Ultra Office Policy employment practices liability: $ 2 million ▪ E&O: $ 2 million	▪ E&O covers theft, misuse and mismanagement. ▪ Employment practice liability covers risk managers.
DHIN*	Sovereign Immunity	See *Impacts of Law and Government*

*Part of AHRQ's SRD in Health IT contracts (AHRQ-04-0015).

†The respondent mentioned that D&O and E&O coverage will be subject to increase in the near future. Negotiations are currently being worked out.

Premiums

There is significant overlap between the factors that influence how much coverage a RHIO obtains and the factors that influence the cost of premiums. In general, the RHIO decides on the level of coverage it needs and then the RHIO's insurer and/or underwriter negotiates the premiums. Traditionally, insurers and/or underwriters calculate premiums based on the revenue and assets of an entity and the identified risks. Given that most RHIOs today are nonprofit entities and have limited or no assets, this approach has significant limitations. The RHIOs included in this report

reported that key determinants for determining premiums used by their insurers and underwriters included:

- Technical architecture: Use of a federated (decentralized) architecture was associated with less risk.
- Data security: Where the data is stored, how many people have access, security provisions in terms of firewalls, intrusion detection, and encryption.
- Type of data being exchanged: The risk associated with the exchange of clinical data was higher than that associated with administrative data.
- Services offered by the RHIO or operational service provider: The higher the number of services offered by the RHIO, the greater the exposure and the higher the premiums and associated coverage.

Other factors identified by some RHIOs included the number of exchange partners, governance, volume of transactions, volume of data being stored, number of patients, and accreditation. While RHIO accreditation is still in its infancy, the UHIN reported that having a high accreditation rating with the Electronic Health Network Accreditation Commission (EHNAC)[29] helped it demonstrate to the underwriter/broker that, by meeting the standards as outlined by EHNAC, the UHIN was at a lower risk.

This report indicates that the annual premiums for the coverage described above varied between $18,000 and $50,000. Even if a RHIO does not own any data or does not manage the data (e.g. the MSeHA and CORHIO), it may still be required to obtain coverage and pay an annual premium ($18,000 in the case of MSeHA). According to respondents interviewed for this report, this premium seems high, given the MSeHA's minimal risk of exposure. However, respondents who represented RHIOs that were engaged in actual HIE operations directly, e.g. HealthBridge, deemed higher premiums suitable. CORHIO indicated that coming to an agreement with the underwriter on the methodology for determining risk—especially as the organization grows from Beta Stage (with no clinical use of PHI) into early operations, then to state-wide operation, and finally to participating

[29] Established in 1995, the Electronic Healthcare Network Accreditation Commission (EHNAC) is a non-profit independent accrediting agency (EHNAC.org). EHNAC currently accredits 45 healthcare networks, including RxHub LLC. Note that the EHNAC accredits a broad category of healthcare networks, and is therefore not limited to the accreditation of HIOs specifically.

in the National Health Information Network (NHIN)—is a potential key component of negotiating an acceptable premium. Respondents, therefore, perceived premiums as too high or too low based on their RHIO's particular level of data ownership, relationship to its IT vendor(s), and its general role in facilitating data exchange among partners.

Participants also reported that, as the RHIO matures and the services provided expand, there may be changes in coverage and premiums over time. Currently very few insurers and/or underwriters have experience with RHIOs; consequently, RHIOs have a limited set of choices. As the market continues to mature, it is likely that the number of underwriters will increase, and the competition may drive prices down. However, other respondents expressed the fear that prices may increase significantly if a precedent is set once a lawsuit takes place.

There are a variety of factors that influence what RHIOs are ultimately able to negotiate in terms of coverage and premiums; however, many believe that insurers and/or underwriters remain reluctant to or unclear about how to insure RHIOs in the absence of revenue, assets, and track record.

IMPACT OF LAWS AND GOVERNMENT

One factor with the potential to change the liability landscape is the involvement of government. Federal and State laws influence RHIO activities and their handling of liability issues. For this reason, most respondents agreed that it is important to be well-versed and briefed about State privacy and security laws and regulations. HealthBridge recently hired a full-time employee to regularly monitor State and Federal laws and regulations for affects on the RHIO's liability and operations. Variation in the State interpretation of Federal regulations such as HIPAA, and the impact of other relevant State laws and regulation necessitate this kind of vigilance. For example, the current New York privacy and security laws are more restrictive than Federal HIPAA privacy and security regulations. In addition, New York State has a data breach law which is applicable to RHIOs in the State. In these cases, the RHIO needs to adhere to the State requirements—often a costly undertaking—,and/or create additional liability considerations that need to be accounted for when RHIOs assess their risks and negotiate for liability insurance with their brokers. The Health Information Security and Privacy Collaborative (HISPC) contractors, funded by AHRQ and ONC, [30] have done significant work in this area. Respondents for this report indicated that in general, States do not have regulations that require the applicability of liability insurance, although Indiana requires RHIOs to have an umbrella of $5 million in liability insurance for general business liability when dealing with State work.

Some respondents indicated that the most effective way that the government can affect a RHIO's liability is by granting the RHIO sovereign immunity. This is best illustrated in the case of public utilities—often formed as private and public collaboratives—such as the DHIN. As a state-wide RHIO, the Delaware General Assembly granted the DHIN sovereign immunity under State constitution, exempting the DHIN and its member organizations from liability risk. Under the DHIN statute, the RHIO will not be held liable except in cases of bad faith or malicious conduct. The statute was created this way largely for the purpose of addressing physicians' liability concerns. The stakeholders spent more than a year discussing legal alternatives and building consensus; trial

[30] AHRQ and ONC implemented a national collaborative effort to address privacy and security policy questions affecting interoperable HIE. Thirty-three states and one territory (Puerto Rico) were engaged to form the initial Health Information Security and Privacy Collaboration (HISPC). The HISPC currently includes the participation of forty-two states and territories.

lawyers lobbied in opposition to giving the DHIN this level of immunity. To further ease physicians' concerns about liability, the DHIN statute states that providers of inaccurate data will be held responsible only if they violate formal rules specified in their contracts. The statute also specifies that a physician's decision to use or not use the DHIN will not affect his or her liability. The DHIN lawmakers hoped that this provision would protect physicians from frivolous lawsuits that accuse them of failure to sort through a patient's entire medical record during treatment. Because of these legislative protections, the DHIN does not require its partners, except for its vendors and contractors, to have liability insurance. Similarly, Rhode Island's law provides immunity to health care providers who rely in good faith upon information accessed through HIE in the treatment of a patient.

Although sovereign immunity may seem like the ultimate solution to liability issues, there are some potentially negative factors that merit consideration. Although immunity was the best option for the DHIN, a few respondents wondered whether sovereign immunity may unintentionally reduce a RHIO's sense of accountability. If faced with legal issues, however, the DHIN would have to answer to the public, which may provide another mechanism for accountability. The DHIN respondents also believed that it might be difficult for larger States to follow the Delaware model for establishing RHIOs because of the effort required to come to a consensus—Delaware's population is less than one million. Overall, the advantages of this model are significant: reduced start-up costs and lower barriers for participants, particularly physicians, to join the organization. On the other hand, one respondent believed that granting RHIOs sovereign immunity would shift liability onto the shoulders of partners and participating members, which are sometimes wealthy private organizations. This would limit the willingness of stakeholders to participate in the exchange.

Several respondents mentioned the potential role of federal and/or state-level RHIO accreditation initiatives on issues of liability coverage. Some believed that establishing accreditation for RHIOs could provide a level of credibility that would make it easier to acquire appropriate coverage. For example, accreditation could be used by insurers and/or underwriters who are assessing the RHIO's level of risk, which would in turn keep the costs of coverage and premiums down. Others contended that accreditation initiatives may be premature and could negatively impact this new and fledgling RHIO environment. To date, the accreditation of RHIOs has been pursued on various levels, including the national Certification Commission for Health Information Technology

(CCHIT),[31] and state-level initiatives such as the New York eHealth Collaborative (NYeC).[32] In August 2008, the independent nonprofit organization Electronic Healthcare Network Accreditation Commission (EHNAC) announced plans to create a RHIO accreditation program, which is targeted to start in 2009.[33] It is important to note, however, that respondents for this report remained divided on their views regarding the role of accreditation and whether accreditation is even feasible at the present time.

[31] CCHIT. Certification Commission. http://www.cchit.org/hie/. Accessed on May 20, 2009.

[32] New York eHealth Collaborative. September 2008. White Paper. Interoperable Health Information Exchange Policy, Governance, and Accountability: Examining the Potential Role for RHIO Accreditation in New York's Health Information Technology Strategy.

[33] ENACH. ENACH To Develop HIE Accreditation Program (August, 2008). http://ehnac.org/pr_2008-0818.html. Accessed on May 20, 2009.

LESSONS LEARNED

This section summarizes the key lessons that may help RHIOs plan a strategy for tackling liability issues.

When shopping for coverage, hire an insurance broker and reach out to your community. Several respondents discussed their approaches to finding the appropriate insurance company, agent/broker, and underwriter. As HIE continues to grow, more and more insurance companies are becoming increasingly acquainted with the amount of liability insurance required to cover a RHIO. According to some respondents, the search for an insurance company was often challenging, although choices have increased in recent years. In order to overcome this barrier, many RHIOs hire an insurance broker or agent to "shop" for the appropriate coverage. An experienced and knowledgeable insurance broker can often serve as an invaluable tool for finding the right coverage. A few respondents mentioned an approach that included consulting with the RHIO's board of directors and existing affiliates or community members for recommendations. Since many of the RHIO's board members and stakeholders are part of the RHIO's health care community, they have often dealt with liability coverage in their organizations and can therefore point the RHIO to various resources.

Plan ahead with the application process. Like any insurance application, the application process can be long and onerous. In addition to its length, the application often asks for a level of detail that will require consulting both the appropriate documentation and other individuals. Insurance should be considered at the very beginning of RHIO efforts, because this will allow the roles and responsibilities of all participating organizations—data sources, users, owners—to be clearly delineated. This is important because liability coverage of the RHIO may largely be determined by contracts with partners. Respondents recommended acquiring coverage at least five to six months before the "go-live" date. It is important not to underestimate the amount of time, resources, and effort that is required to apply for coverage; planning well ahead of "go-live" will reduce the risk of the application being pushed through hurriedly after the RHIO has begun exchanging data. Respondents mentioned the need to be complete, detailed, and thorough with the application in order to verify that there are no gaps in coverage and that all the appropriate provisions are included in the application. Appendix C is a set of sample questions from an insurance application form.

Be prepared to educate the insurance brokers and/or underwriters. Once RHIOs have researched their options and decided on a particular underwriter, they also need to educate the underwriters on the way RHIOs work. Respondents mentioned that they had to sit down and meet with the underwriter to explain various aspects of the RHIO, including governance, privacy and security, and technical architecture. Many respondents noted that the insurance application contained questions that seemed irrelevant or had minimal applicability to RHIOs. This is largely because many underwriters do not conduct a formal review of the RHIO's environment before underwriting the policy. In the case of the RIQI, the RHIO will be responsible for the management of data following transfer from the Rhode Island Department of Health, but EDS, their future IT vendor, will be responsible for the storage and technical infrastructure that supports the data.[34] The insurance application, however, asked the RIQI specific questions about the security of the way the data was stored, questions which may have been better suited for the vendor. Every RHIO also has a unique set of participating agreements with partners, and the underwriting process needs to be tailored according to these factors. One respondent stressed the importance of describing specific scenarios to the underwriter. Many State and regional differences make the underwriting policy difficult to generalize and standardize on a national level.

Know State and Federal regulations. It is important that the RHIO's board of directors and management are well versed and briefed in the current state of the industry. In particular, an understanding of the RHIO's State regulations, as well as State interpretations of Federal regulations, is necessary in order to track the possible impact of these trends on RHIO activities. Many respondents believed that actively researching and being vigilant about trends in regulations are vital to assessing the RHIO's changes in coverage needs over time. If State interpretations of HIPAA become increasingly restrictive, as in New York for example, the RHIO's E&O coverage will need to be expanded.

Identify gaps in coverage. It is important to understand that underwriters and insurers may not capture all the pitfalls and loopholes of coverage. The RHIO must verify that there are no potential gaps in coverage. With a council of legal advisors, the RHIO will need to ensure that the coverage considers all of the RHIO's factors, State and Federal regulations, and any other potential scenarios

[34] EDS is the Rhode Island Department of Health's IT vendor. The technical oversight and management of the RHIO will be transferred from the Department of Health to the RIQI in 2010.

in which the RHIO could be left liable. A thorough and meticulous examination of coverage is important. Given the uncertainty of the level of risk among RHIOs and the lack of precedent, most respondents held the belief that "over" covering is better than "under" covering.

Expect some administrative burdens. Most respondents reported that managing current coverage—renewing the policy annually—is not an administrative burden. There are, however, administrative burdens associated with educating the underwriters, expanding current coverage, and undergoing certification processes in order to maintain coverage and premiums at a low cost.

Insurance policies must be tailored to your RHIO. RHIOs differ widely in terms of governance, technical architecture, relationship with exchange partners, scope of services, and cultural and business practices. As a result, all RHIOs have different ways of dealing with liability insurance issues. A common theme that emerged among respondents is that the insurance policy must be tailored to the unique circumstances and characteristics of the RHIO. Until there is a conjoined effort to create a master insurance policy to address RHIOs' common liability insurance concerns, RHIOs liability insurance efforts will remain a reflection of distinctive local and community activities.

As a summary of the various lessons learned, the following key steps to acquiring an insurance policy for a RHIO were extracted from our discussions with representatives in the field:

- **Reach out.** Reach out to community stakeholders for guidance and advice.
- **Plan ahead.** Factor in the potential administrative and financial burdens of purchasing a policy.
- **Hire.** Hire an experienced insurance broker to shop for the right policy and help negotiate premiums.
- **Know the industry.** Understand the current state of the HIE industry and the implications of government regulations on your RHIO's liability.
- **Educate the underwriter and/or broker** on RHIO fundamentals including the services it offers and its technical architecture.

- **Build consensus among partners** on liability distribution.

- **Complete the required documentation**. The insurance application form can be extensive, requiring a high level of detail and a significant expenditure of time and resources.

- **Negotiate the terms of the policy**, including premiums and the amount of coverage needed. An insurance broker can be invaluable in this process.

- **Identify gaps in coverage.** With the council of legal advisors, verify potential oversights in coverage.

CONCLUSIONS

The importance and weight of liability issues varies among RHIOs. In some instances, concerns over liability determined the legal and governing status of a RHIO, as in the case of the DHIN; and in others, the ability to leverage existing liability practices of larger governing entities reduced liability concerns, as in the case of the INPC because of its connection with the Regenstrief Institute. Some respondents shaped their policies and MSDAs around liability issues, while other respondents believed that HIE should not add any more substantial liability than paper-based information exchange. These variations reflect the lack of standardized liability practices to date.

Obtaining liability coverage takes a considerable amount of time. While each of the RHIOs approached the issue of obtaining insurance differently, they all spent considerable time identifying the risks and accountability of the various participants, looking for and settling on an underwriter, and educating the underwriter on HIE. While almost all the RHIOs included in the report had liability insurance in place prior to "going-live," the planning process varied considerably and was influenced by stakeholder involvement, the technical architecture of the exchange, the services performed by the RHIO, and the services provided by the IT vendor and/or the operational service providers. At a minimum, most RHIOs obtain D&O and E&O insurance. In some cases, RHIOs also obtained employers' insurance and security and privacy liability policies. The different policies that a RHIO obtains is influenced by State laws on privacy and security and, if applicable, any specific State laws on RHIO immunity.

There remains a high degree of legal uncertainty. Our examination of liability insurance practices revealed that this is still a relatively new and emerging area. Given the lack of a precedent on how courts would approach a privacy or security breach, there is little clarity about who would ultimately be held liable. RHIOs have tried to address this in various business contracts with partners. Many respondents predicted that in the case of a mishap or breach, most, if not all, parties will ultimately be held liable. The lack of any court precedents similarly results in the absence of reference points for RHIOs' advice to attorneys and insurance brokers. These uncertainties have a wide range of effects on RHIOs, from increasing premiums to increasing incidents of overlapping liability coverage among various RHIO participants. Despite the current level of legal uncertainty and variation of liability practices in the field, our discussions with various RHIOs and HIE liability

insurance representatives have lead to a greater understanding of how these legal uncertainties can be overcome.

Insurance policy options for RHIOs are growing but remain limited. While the number of brokers and underwriters continues to expand, the options for RHIOs remain limited. The traditional model used by underwriters is based on identifying an entity's assets and quantifying its risks. Given that most RHIOs are nonprofit organizations with limited if any assets, underwriters must consider other factors such as technical architecture, services provided, types of data being exchanged, and security controls for stored data.

There is wide variability in liability insurance practices across RHIOs. Our findings revealed that there are considerable variations in liability insurance. Variability in liability insurance practices are a reflection of both an emerging landscape of HIE and the unique local and regional communities from which RHIOs emerge. There are a limited yet growing number of operational RHIOs to date; each RHIO possesses its own variation of organizational structure and governance, technical approaches, and services provided to meet the unique demands of the community or region it operates in. Consequently, liability insurance practices substantially vary across RHIOs.

Sovereign immunity has its advantages and disadvantages. Respondents remained divided on the role of the State or Federal government in offering immunity to RHIOs and its partners. While some respondents were strong proponents of State immunity, citing such benefits as increased stakeholder participation, decreased start-up costs, and long-term sustainability; other respondents seemed skeptical and noted that if State immunity is available, RHIOs may not be as rigorous in establishing privacy and security controls. One respondent strongly believed that both State and Federal legislatures should work with the health care community to create a level of immunity that encourages the participation and facilitation of HIE. Another respondent, however, mentioned that providing sovereign immunity to a RHIO would decrease initial stakeholder buy-in because potential partners would interpret the RHIO's immunity to mean that stakeholders will be more likely to be targeted in a lawsuit. A RHIO's partners would therefore need to be granted legal immunity as well. In such a scenario, however, a patient would not have much legal recourse in the case of harm or injury as a result of the negligent actions of an immune RHIO or its partners.

Although RHIOs may continue to experience challenges in obtaining liability insurance, there are growing examples of RHIOs that have been able to obtain insurance and can provide important lessons on how to navigate this complex and uncertain landscape.

APPENDIX A
RHIOS, RESPONDENTS, AND RESPONDENTS' TITLES/ROLES

RHIO	*Respondents*	*Title/Role*
Rhode Island Quality Institute (RIQI)	Judith Wright	Vice President
Delaware Health Information Network (DHIN)	Gina Perez, Paula Roy, & Marc Niedzielski	Executive Director (ED), DHIN; ED, Delaware Health Care Commission (DHCC), and Deputy Attorney General
Utah Health Information Network (UHIN)	Shaunna Wozab	Project manager
Colorado Regional Health Information Organization (CORHIO)_	Phyllis Albritton, Stephen Nash, and Sarah Stevens	Interim Executive Director, CORHIO; Partner at Holme, Roberts, & Owen, LLC; and Aon representative
Indiana Network for Patient Care (INPC)	Marc Overhage	Director of Medical Informatics and Research Scientist, Regenstrief Institute, Inc.; President, CEO, Indiana Health Information Exchange
MidSouth eHealth Alliance (MSeHA)	Vicki Estrin	Program Manager
Taconic Health Information Network Community (THINC)	Susan Stuard	Executive Director
HealthBridge	Keith Hepp	VP of Business Development, CFO
Others	Stephen Bernstein	Attorney at McDermott Will & Emery, LLP
	David Hartzband	Founder & Principal of PostTechnical Research, visiting scholar at MIT
	Chris Philipps	VP of insurance division at City Securities Corporation
	Brandon Wellford	CFO at Memphis Bioworks Foundation

APPENDIX B
QUESTIONS FOR DISCUSSION

Background question: For what purpose(s) does your RHIO share data?

Q1: Who are all of the entities that currently take on liabilities because of participation in your RHIO? Some examples listed below

1) RHIO organization and board of directors
2) RHIO employees
3) Government
4) University
5) IT vendors
6) Partnering organizations – data sources
7) Partnering organizations – data users
8) Payers
9) Other contracted partners

Q2: What are all of the possible categories of liability coverage relevant to your RHIO? (Please indicate standard categories if they exist.) Possibilities are listed below.

1) Data theft
2) Data mismanagement (e.g., software or hardware error resulting in use of incorrect data, unavailability of data, permanent loss of data, accidental disclosure of data resulting in reduced quality of care, data disclosed to unauthorized party)
3) Data generation error (e.g., incorrect, incomplete or otherwise poor quality data from source, failure to update or correct faulty data, resulting in reduced quality of care.)
4) Data misuse (e.g., correct data misinterpreted at time of care)
5) Directors' and officers' liability
6) Others?

Q3: What level of coverage does your RHIO have for each of the categories mentioned (or whatever categories are used), and what does the coverage cost?

Q4: Do you require partners to carry insurance? If so, what level of insurance are partners required to carry?

Q5: In your best assessment and based on your experience, which factors affect the above levels of coverage required and by how much?

1) Number of partners
2) RHIO revenue
3) Number of patients
4) Number of bytes of data stored by RHIO
5) RHIO technical architecture
6) Others

Q6: How are these levels of coverage and costs of liability insurance expected to change as the RHIO grows? Is there a certain size above which the liability will escalate severely? Should the liability shift over time? (For example, should the vendor have higher liability in the first year because of the experimental nature of these products?)

Q7: At what stage in development did you start planning for liability insurance?

Q8: How did you go about finding an underwriter? What were some of the challenges you encountered?

Q9: How significant do you find the administrative burden of managing liability for the RHIO? What are the key factors that increase the burden?

Q10: In your State are there any existing State laws that are relevant to RHIO liability?

Q11: In your assessment, how might various liability distributions influence RHIO organizational structure, technical architecture (central, hybrid, federated) and other RHIO decisions? (Or is the direction of causality the reverse?)

Q12: Are there any limits on who can provide data and who can access the data? Did liability concerns influence these limitations? If so, how?

Q13: What were the top three to five lessons that you can share with respect to acquiring liability insurance for your RHIO?

Q14: To what extent does government liability coverage enhance or limit the RHIO's organizational development and potential? (Answer if applicable.)

Q15: What are the advantages and disadvantages of having sovereign immunity? Should RHIOs lobby for this immunity in every State? At the Federal level?

Q16: What are the advantages and disadvantages of shifting liability to larger organizations such as Universities and government? Do those organizations demand strict, cumbersome oversight?

Q17: Is there anyone else you recommend we speak to with regard to this issue? Are there any other resources you can point us to?

APPENDIX C
SAMPLE QUESTIONS FROM SECTION 4 AND 5 OF DARWIN'S PRIVACY LIABILITY AND NETWORK RISK INSURANCE APPLICATION

4. NETWORK SECURITY

(a) Are firewalls in use within the Applicant organization?

☐ Yes ☐ No

If "Yes," please outline the brand, model number, and portion of the Network each firewall is protecting.

_____

_____

(b) Are Intrusion Detection Sensors or Intrusion Prevention Sensors (IDS/IPS) in place throughout the Applicant's Network?

☐ Yes ☐ No

If "Yes," answer the following:

Identify the sensor brand and model:

_____

Explain where the IDS/IPS are located:

_____

(c) Is an Event Response Plan in place for dealing with IDS/IPS events?

☐ Yes No

(d) How frequently are the firewall and Intrusion Detection System rules sets updated?

_____

(e) Excluding firewalls and IDS/IPS, detail all other technical security devices currently protecting the Applicant organization's Network (e.g. content firewalls, other monitoring devices etc):

_____

_____

(f) Does the Applicant have consistent security standards for network endpoints?

☐ Yes ☐ No

(g) Are Wireless Access Points (WAPs) available within the Applicant's environment?

☐ Yes ☐ No

If 'Yes," explain the role that WAPs serve within the Applicant organization:

_____

_____

Describe any security mechanisms currently in place for WAPs:

_____

_____

_____

(h) Does the Applicant have a hard-drive destruction policy in place?

☐ Yes ☐ No

If "Yes," explain the process:

_____

_____

_____

(i) Are data leakage controls or applications installed to prevent accidental dissemination of confidential information (such as email or FTP scanning)?

☐ Yes ☐ No

If "Yes," identify controls or applications in place:

_____

_____

(j) Has the Applicant organization conducted penetration testing?

☐ Yes ☐ No

If "Yes," identify below the focus of the penetration testing:

Network based_____ Application based_____

Social based _____ Other (specify): _____

Provide the names of the companies/vendors performing the last three penetration tests for the Applicant and the associated dates of the tests:

_____

_____

_____

_____

(k) Does Your Data Center hold any active certifications (e.g. SAS 70, ISO 17799 adherence)?

☐ Yes ☐ No

If "Yes," please list:

:_____

_____

_____

_____

(l) Does the Applicant organization employ regular vulnerability scanning?

☐ Yes ☐ No

If "Yes," when was the last scan performed?

_____

What product was used to perform the scan?

_____

If a vendor performed the scan, what vendor?

_____

Have all critical deficiencies been addressed by Applicant?

☐ Yes ☐ No

If "No," list deficiencies not addressed:

_____

_____

_____

5. ANTI-X DEFENSE (ANTI-VIRUS, ANTI-SPAM, ANTI-SPYWARE)

(a) Detail the Applicant's anti-virus, anti-spam and anti-spyware applications, any vendors used, and the update frequency for each component:

_____

_____

_____

_____

(b) Has the Applicant organization experienced any virus infections or spyware/malware infections in the past two years?

☐ Yes ☐ No

If "Yes," please provide the following information:

1. What length of time was required for remediation?

_____

2. How many workstations/servers were compromised by the infection?

_____

3. How have defenses been bolstered since last infection?

_____

_____