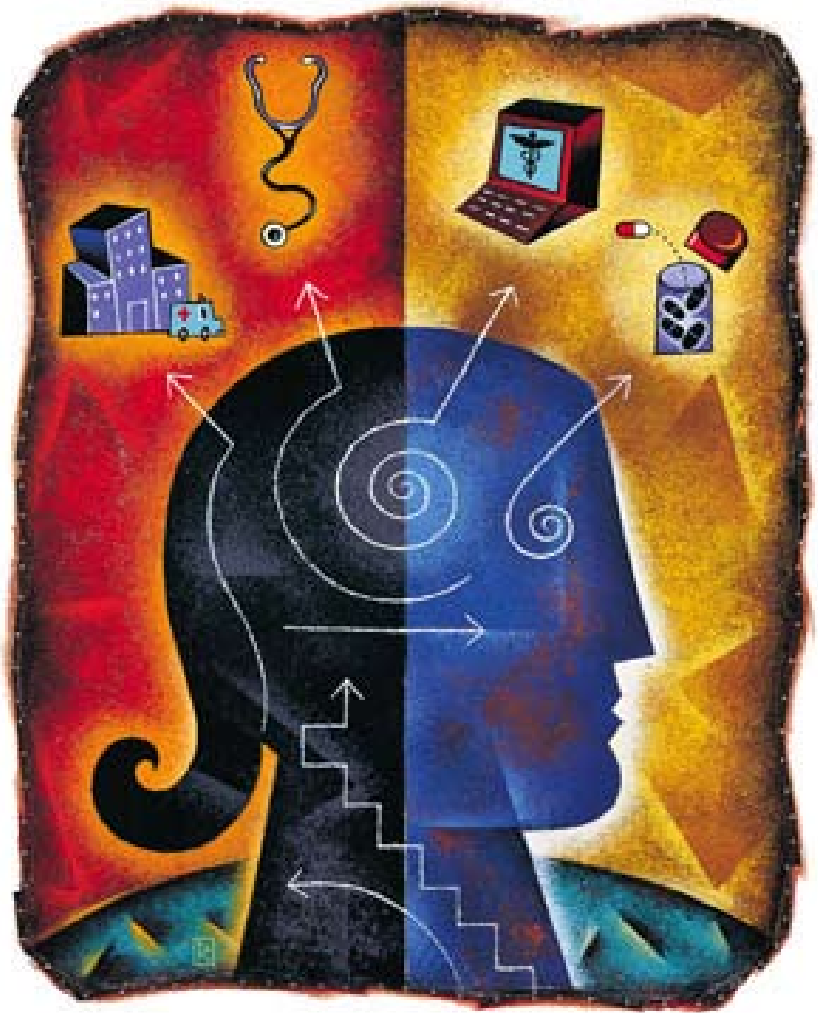
California HealthCare Foundation



Privacy, Security, and the Regional Health Information Organization

ihealthreports

June 2007

Privacy, Security, and the Regional Health Information Organization

Prepared for
California HealthCare Foundation

by
Sheera Rosenfeld, Shannah Koss, and Sharon Siler
Avalere Health LLC

ihealthreports

June 2007

Acknowledgments

The authors thank all of the organizations that participated in this project for sharing their experiences and insight.

About the Authors

Sheera Rosenfeld is a director, Shannah Koss is a vice president, and Sharon Siler is a senior associate at Avalere Health LLC, focusing on health information technology and exchange issues. Avalere Health provides strategy, research, and educational products to a range of commercial and non-profit customers with interests in improving the health care system.

About the Foundation

The **California HealthCare Foundation,** based in Oakland, is an independent philanthropy committed to improving California's health care delivery and financing systems. Formed in 1996, our goal is to ensure that all Californians have access to affordable, quality health care. For more information about CHCF, visit us online at www.chcf.org.

ISBN 1-933795-29-8

Contents

I. Executive Summary

Regional health information organizations (RHIOs), which promote electronic exchange of patient information among participants, are in the early stages of development. As they grow, RHIOs must establish policies and practices to protect the privacy and security of that information, an often difficult undertaking.

This study, based on a literature review, interviews, and an informal survey, examines key privacy and security issues that some RHIOs encounter, the policies and practices they adopt to manage these issues, and common emerging strategies.

The study finds that privacy and security challenges are surmountable. A RHIO's unique characteristics—the types of data shared, who participates, its specific needs and priorities, and other factors—influence how an exchange addresses these challenges. Solutions are diverse and evolving. The study also finds that consumers play a limited role in privacy and policy decisions, even though they are important RHIO constituents. Nascent exchanges could benefit from the experiences of and collaboration with others, and policymakers can help RHIOs navigate privacy and security issues and move toward sustainability.

RHIOs are more likely to overcome privacy and security challenges if they avoid narrow privacy and security solutions, address external factors such as legal requirements and community priorities, and engage a broad range of constituents. They should also use existing privacy and security frameworks as a starting point, anticipate long-term infrastructure needs and goals, and consider how they can become sustainable over the long term.

II. Introduction

Resolving privacy and security issues is essential in forming, governing, and operating regional health information organizations. RHIO participants, including consumers, must feel confident that personal health information is private and secure, and that all exchanges of information meet legal and ethical requirements. Most RHIOs are evolving and many continue to struggle with these challenges, although common strategies for meeting them are beginning to surface.

Avalere Health conducted research and interviews to better understand some of the key privacy and security issues RHIOs face, including how such issues affect RHIO development and operations, how significant the challenges are, how RHIOs are managing those challenges, and the types of best practices that are emerging. This report:

- Identifies key privacy and security questions that RHIOs must consider.
- Discusses how privacy and security issues may influence the planning and implementation of RHIOs and the support of participants.
- Examines current privacy and security policies.
- Considers the consumer perspective and level of consumer engagement in privacy and security issues.
- Recommends steps RHIOs and others can take to overcome the related challenges.

III. Background

Health information exchange initiatives first emerged in the mid- to late-1980s as community health information networks (CHINs). CHINs achieved some success through the mid-1990s but ultimately failed because of organizational and implementation issues, including a lack of standards and funding and poor technical infrastructure.[1–4] Rapid advances in information technology, an industrywide focus on standards, and the ability of different computer systems to share information have enabled health information exchange to come to the forefront.

RHIOs typically provide one or both of two core services: the governance body and policies for facilitating information exchange among participants and the technical infrastructure for automated exchange. Increasingly, they formally oversee and govern information sharing, and they often shape policy and direct decision-making—for example, by convening committees or workgroups to address privacy and security issues and by designating board members to lead these activities.

Although RHIOs often start out informally or as part of existing public or nonprofit organizations, most anticipate establishing stand-alone entities that may have nonprofit, 501(c)(3) status under the Internal Revenue Code.

A RHIO consists of physicians, hospitals, health plans, laboratories, consumers, and others who seek to share electronic health information about patients in a community, state, or region. Each RHIO is unique, based on the needs and characteristics of the community it serves.[5] Medication, lab, emergency, and administrative data are the most common types of information that RHIOs initially plan to exchange. They also may offer additional capabilities, such as data storage.

Benefits of Information Exchange

Among the benefits of RHIOs are higher quality of care, more efficient delivery of services, safer patient care, and overall cost savings. Greater availability of clinical information at the point of care can reduce duplicate services and administrative follow-up, such as requests for patient records or clarification of prescriptions; reduce adverse drug events; and promote better coordination

of care. Information exchange also can facilitate preventive care and disease management, and, for providers, foster a better understanding of specific treatment protocols, drug regimens, and related outcomes.

The Federal Role

The federal government is promoting, and reducing the barriers to, health information exchange in part by harmonizing standards and certifying criteria for electronic health records.

See Appendix A for details about specific initiatives and activities.

Improvements in quality and efficiency can save money. Potential annual savings—between $70 and $80 billion[6–8]—will largely accrue to payers and depend on how quickly providers adopt health information technology and participate in data exchanges.

RHIO formation is largely driven by the interests of participants, what they believe will benefit their community, and a relatively quick demonstration of a strong business case. The type of information exchange, the community's needs, the kinds of participants, the previous relationships and level of trust among them, and the backgrounds and perspectives of those who lead the organization—vendors, clinicians, or researchers—all determine how a RHIO makes privacy and security decisions.

Nationwide, more than 100 health information exchange initiatives are under way, most of which focus on patient-level clinical information.[9] However, many initiatives are still in the planning or early implementation stages. Few RHIOs currently exchange data, and even fewer have been exchanging multiple data sets for more than a year.[10,11] Many expect to continue expanding their scope by adding new participants and types of shared data.

Common Issues

Throughout their evolution, RHIOs must address four critical issues that will largely determine success:

Financial. These are the most challenging. They include overcoming the high up-front cost of technology systems, aligning incentives for participation, developing a strong and common value proposition for all stakeholders, and creating a sustainable revenue model.

Cultural and organizational. Such issues often include workflow and productivity disruptions, fear that health plans will prematurely use data in pay-for-performance programs, and participants' competing priorities and demands on time.

Technical. These issues range from participants' different levels of technical sophistication and information technology expertise to the inability of information systems to exchange data because the data are inadequate and exchange standards are lacking.

Privacy and security. All RHIO stages involve privacy and security issues, the complexity of which varies. These include concerns about the confidentiality of patient information and questions about who should have access to it, how the information will be used, and the technical safeguards in place to secure it.

Privacy, Security, and HIPAA

Privacy and security are related but distinct issues. Privacy is the protection of patient health information due to its sensitive and confidential nature. Security is the means by which organizations ensure the availability, confidentiality, and integrity of that information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets the backdrop for how RHIOs deal with privacy and security. However, most RHIOs are not directly subject to HIPAA's requirements.

See Appendix A for more information about HIPAA.

IV. Methodology

To further understand current and future issues regarding privacy and security, Avalere Health reviewed the literature, interviewed representatives of nine mature RHIOs and two privacy experts (Appendix B), and informally surveyed other RHIO representatives. Most of these RHIOs are operating; others have nearly completed a pilot phase or are at the end of a planning phase.

Over four months, Avalere Health developed and used a structured guide for interviewing the nine RHIO representatives about their privacy and security policies and practices, and related issues. Questions focused on how privacy and security concerns have influenced participation in their exchange organizations, how difficult it was for their RHIOs to develop privacy policies, whether the exchanges used any existing policies as models, and how federal privacy and security activities affect their day-to-day operations.

Using this guide, the authors also asked representatives of several other exchanges to complete an informal written survey. For the consumer perspective, the authors interviewed two consumer privacy experts.

V. Findings

Most RHIOs, which must ensure that safeguards are adequate to protect data exchange, are working to build trust within their health care communities. The literature and anecdotes suggest that privacy and security present substantial challenges and even barriers for most developing or operational RHIOs. Understanding the extent of such challenges was a primary goal of this study.

Highlights

The most significant insights about privacy and security policies and practices and how they affect RHIO planning, implementation, and operations include the following:

- While privacy and security are important issues, interviewees did not consider them insurmountable. Still, privacy and security directly affect an array of key RHIO decisions, must be carefully considered and managed, and may ultimately impact community trust and the willingness of certain constituents to participate in information exchange.
- RHIOs' privacy and security practices are evolving and vary. Even as such practices mature and become more defined, they will continue to change as RHIOs expand the type of data exchanged and as the number and types of participants grow.
- The significance of privacy and security, the related challenges, and the ways that policy and technical issues are addressed depend on a RHIO's unique characteristics, particularly on the kinds of data being exchanged and types of participants involved.
- Although the privacy and security issues RHIOs must address are similar, approaches vary significantly. RHIOs must scale policies and procedures to the needs, sizes, and types of participants. While maintaining privacy and security, they also must allow some flexibility in each participant's approach to these issues.
- Consumers remain on the sidelines when it comes to developing RHIO privacy and security policies and practices. They and consumer advocates are more concerned about these issues than

RHIOs are because privacy and security have a direct personal impact.

- There are privacy and security models and lessons learned that could guide nascent RHIOs, such as using HIPAA as a starting framework. By collaborating with other exchanges, evolving RHIOs could benefit from existing privacy and security policies and practices, and from successful strategies for implementing them.
- Federal and state policymakers can play a supporting role for RHIOs and help them achieve their long-term goal of sustainability. In particular, they can clarify HIPAA, evaluate the barriers to secondary uses of data, look at ways to overcome those barriers, and continue to foster shared learning among exchanges.

Four Key Questions

All nascent RHIOs must address four fundamental questions: Who will have access to patient information? Which information will be accessible? What are acceptable purposes of exchange? And under what circumstances should users be able to access information?

The questions are closely related, as the approach a RHIO takes to one issue often directly influences its approach to others. Moreover, as RHIOs continue to evolve, expand the kinds of data exchanged, and increase the number and types of participants, they must ask and answer these questions repeatedly. Given the rudimentary nature of most RHIOs, resolving an issue may be difficult.

Who Will Have Access?

Often, a RHIO must decide which entities, but also which individuals within those entities, will have access. And the RHIO must determine what level of access will be necessary to support its data exchange goals.

Some exchanges decide who will have access based solely on the potential users' role in direct patient care. At nearly all of the RHIOs in this study, physicians first and foremost have consistent access to patient information. Other commonly authorized users are employees of participating hospitals—registered nurses, pharmacists, and registrar and medical-records staffers, for example—and those who work in physician offices, such as registered nurses, physician assistants, and administrative staff.

To Give but Not Receive

Many RHIO participants are not authorized to access data that health care providers generate. For example, some RHIOs permit certain constituent groups, such as health plans or employers, to give but not receive data. Concerns about the potential use of data for performance measurement and oversight, rather than about patient privacy, may drive these limitations.

Interviewees noted that, despite some differences of opinion, giving access to users directly involved in patient care was generally not contentious. However, reaching consensus on secondary uses of data was more challenging. According to some interviewees, secondary-use issues generated concerns about privacy and security, as well as significant controversy, particularly regarding information access for payers, ancillary providers, and others who were not physicians or on a physician's staff, or who did not treat patients directly. A small number of interviewees suggested that the type of participants who were the leading constituents in a RHIO—most often physicians and hospitals—had greater influence on deciding who would have access than any specific privacy concerns did.

Which Information Will Be Accessible?

Which data to exchange, be they lab results, medication history, and/or admission and discharge information, often is determined in the early RHIO stages. In many cases, such decisions depend on which information is easily accessible, is readily available, and provides immediate value at the point of care. Interviewees indicated that common initial data exchanges included lab results, medication

history, and clinical records for emergency department admissions. Privacy and security issues often dictated more detailed or explicit decisions than other issues did. One issue, for example, was whether only part of a clinical record, such as demographic information, could or should be viewed and exchanged.

Although they define and determine access to specific data in different ways, most RHIOs are driven in part by the "minimum necessary" standard under HIPAA, which governs and sets a floor for most use and disclosure policies. The premise of this standard is that physicians, hospital clinical staffers, administrative staff members, and others should have access only to the minimum amount of personal health information necessary. Such decisions determine not only which data will be exchanged, but also which will be explicitly excluded.

Nearly all interviewees said their RHIOs explicitly exclude sensitive patient data—including information about mental health, substance abuse, and HIV/AIDS—from their exchanges. Most acknowledged the challenge of total exclusion, given that many diagnoses can be inferred from medication lists or lab tests. Many states have laws protecting certain types of patient data, yet these laws did not appear to be the primary stimulus for RHIOs' strict access rules; rather, deeply rooted ethical concerns about inappropriate access, the sensitive nature of the information, and the concerns of patients and patient advocacy groups tended to drive such rules.

Information Access Policies

These may define "read only" or "read and add." The latter means an authorized user can supplement the existing record with notes, results, or other information but cannot edit, alter, or delete anything. Access is often time-limited: Users can access patient information only during an episode of care.

What Are Acceptable Purposes of Exchange?

This is a core issue for nascent RHIOs, one influenced to varying degrees by privacy and security concerns. Interviewees said their RHIOs were able to establish, without controversy, rules for using data in clinical treatment and that they usually imposed disclosure limitations consistent with HIPAA and state laws. However, when potential purposes included secondary uses, such as conducting clinical research, measuring performance, improving population health, and marketing, consensus was sometimes unattainable.

The extent to which participating organizations use RHIO data for their own institutional purposes other than treatment tends to generate considerable discussion and concern. Interviewees mentioned such use, but none said his or her RHIO authorized it specifically to support marketing. And few cited research or other uses as a primary purpose for initial information exchange.

Some RHIOs increasingly view clinical research, in particular, as a legitimate and potentially revenue-generating secondary use. Those affiliated with an academic medical center or research institution may be more interested in and willing to accept such use.

What Circumstances Justify Exchange?

The circumstances under which RHIO participants can access and exchange data drive the design of infrastructure, processes, and safeguards. Policies specify those circumstances and how security measures will protect privacy.

Once RHIOs answer these four questions and have a clear set of privacy and security principles in place, they can begin exploring policy solutions to ensure compliance and adherence.

Business Associate Agreements Ensure Compliance

Because most RHIOs are not subject to HIPAA, business associate agreements are the primary way they ensure that participants will comply with an exchange's practices and data exchange requirements. These agreements:

- Specify how the RHIO will handle and use data.
- Specify how it will notify patients about privacy practices.
- Define participants' roles and business arrangements in the exchange.
- Clarify privacy and security policies.
- Make it easier to put the policies in place.

The agreements can be more or less prescriptive when it comes to privacy and security protections, depending on what the participants believe is appropriate.

VI. Privacy Policies and Practices at Emerging RHIOs

The RHIOs in this study are at various stages of developing and implementing privacy and security policies and practices. Some have adopted the internal policies and practices that participants already had, while others have required that participants make them more robust.

The presence or absence of policies a RHIO has and their types seem to be linked to the RHIO's maturity, sophistication, and level of community engagement. They are influenced by the RHIO's interpretation of HIPAA and applicable state laws, the kinds of participants in the exchange, and how open its policy process is.

Most interviewees did not cite privacy as an insurmountable barrier to RHIO development, but they did say that developing policies on data-use limitations, patient consent, patient access, and authentication of users were significant challenges.

Privacy Policies

Information use and disclosure, which a business associate agreement often defines, are the "rules of the RHIO road"—the broad parameters for information exchange. Many interviewees said they support the use and disclosure policies of hospitals in their RHIO; each hospital adheres to its own policies—for example, giving doctors access only to data about patients for whom they are the physician of record.

One interviewee characterized this approach as following the "rules of the people who control the data." Most said participants' own policies control how they use data created in-house, although at least one indicated that the RHIO's policies govern the exchange of data among participants.

Regardless of the model, exchange members may have inconsistent and sometimes conflicting data-sharing policies. Most of the RHIOs in this survey have not confronted such conflicts or they trust that participants will adhere to HIPAA and ensure sufficient protection.

Patient-consent policies define patients' right to choose whether they want to participate in data exchange. A related issue is whether

patients should have the right to control or prohibit access or use of some personal health information, such as that regarding mental health treatment.

Developing patient-consent policies is difficult because of sensitivity about patient privacy and patient control of data, tension between the desire to improve care and patients' concerns about loss of privacy, and patients not understanding how the RHIO will use their information. Concerns also may stem from a fear that broader automated access poses greater privacy risks. For several RHIOs, patient-consent policies were among the most contentious privacy issues they addressed.

There are three main approaches to patient consent and inclusion of personal information in data exchange: opt-in, opt-out, and no-opt (see sidebar). Only one RHIO chose opt-in, citing community concerns and state law. Most RHIOs use opt-out, and only one has a no-opt policy.

Legal issues aside, many RHIOs and their communities feel strongly that informed consent and educating patients about how the organization will manage information disclosure according to patient preferences are important in forming a RHIO and building its culture of trust and communication. (One way to inform patients about data exchange is to give them standard HIPAA and privacy-notification forms. Depending on the model, a RHIO may be able to accommodate a mix of consent approaches.) Many stressed that this can encourage the participation of providers, at least initially, because they are not forced to change their policies.

Most RHIOs in this study do not let patients set limits on what portion of their personal data will be available for exchange, nor do they give patients direct access to that information through the organization. In some, however, patients may have access to their information through a personal health record. Additionally, some of the RHIOs may give patients authority to limit which data will be released to entities outside the organization but not which data will be widely exchanged within it.

Many RHIOs aspire to give patients access to their own information, but few have policies and technology in place to do so. Some did not have a policy governing patient access to RHIO-based data and have not formally addressed the issue. As mentioned earlier, most of the RHIOs exclude highly sensitive information from exchange, but such exclusion is part of their overall policy.

Privacy Practices

A common way to protect patient privacy is to authorize access to patient information based on the user's role in an organization. This specifically meets the HIPAA standard of releasing only the minimum amount of information necessary to provide care. Many of the RHIOs in this survey employ role-based access to ensure adherence to their use and disclosure policies. Exchange participants—frequently hospitals or physicians in group practices—set the rules for their employees' access.

The way RHIOs and participating providers interpret and implement role-based access varies. Several allow hospitals' internal policies to govern in-house use of patient data. For example, registrars at one hospital are authorized to view all data collected while a patient is in that facility, but they may have access to only limited data, such as demographic information, if the same patient is in a different hospital. A similar policy might apply to physician offices. While providers in all of the RHIOs have access to at least some patient information, physicians may be able to view only the information about patients they treat directly rather than information about all patients, depending on the specific provider, the user's role, or RHIO policy.

Interviewees indicated that their RHIO infrastructures can accommodate the different rules and types of user access.

Protocols for patient recourse must be in place to deal with instances when information is inappropriately disclosed. While RHIOs strive to maintain the privacy of patient information, breaches are likely to occur. The potential for a patient to be adversely affected by the misuse of sensitive information is high.

The interviews revealed that how RHIOs define, develop, or manage consumer remedies in the event of a privacy breach is inconsistent. Several interviewees indicated they are focused on this issue and working to develop a comprehensive policy, but "are not there yet." Many of the RHIOs are aware of the basic HIPAA requirements, but they have not defined or implemented practices that are more stringent or meaningful to consumers. Other interviewees said their RHIOs allow participants to develop and adhere to their own internal policies. Interviewees did not typically cite this as a challenge. Given the variation and immaturity of some policies, many RHIOs may not have sufficiently discussed or fully considered the fundamental breach and mitigation issues.

Procedures for addressing and managing security breaches are critical because RHIOs are custodians of sensitive data. As business associations, they are obligated to notify participants if data transmission or storage is breached. Several interviewees said their organizations take a "federated approach": They defer to participants' privacy-breach procedures. However, some stressed that this method limits RHIOs' ability to ensure that breaches are addressed promptly and means the organization must rely on individual exchange participants to establish and enforce appropriate policies.

Patient-Consent Models

Opt-In. Health care providers must obtain explicit written consent from patients to include their personal health information in a RHIO. The information is included only if the patient so chooses. This model often is the most burdensome and challenging for a RHIO. It ultimately may limit the number of participating patients and the availability of data.

Opt-Out. Patient information is assumed to be included in data exchange. Patients may elect not to participate, but they must explicitly request that their information be excluded. Depending on RHIO policy, they may have to opt out at the individual-hospital or physician level or opt out at the RHIO level. The burden is not on the RHIO to enlist patients, which makes inclusion simpler and less costly. Typically, the opt-out approach means more patients and more data are automatically included in the exchange.

No-Opt. Patient information is assumed to be part of the exchange for treatment purposes only. Patients do not have the option to include or exclude their data. Under HIPAA, patients are not required to consent to data exchange for treatment purposes; therefore, a no-opt approach is legal under federal law, although it may not be permissible under some state laws. If a RHIO wants to use patient data for secondary purposes, such as research, the no-opt approach is more problematic.

Interviewees highlighted several other approaches, such as requiring immediate notification of the affected hospital's HIPAA officer and forcing immediate removal of the faulted user's access to information. Several RHIOs are developing or revisiting their security-breach policies. Most interviewees said they do not view this task as challenging.

HIPAA Flexibility

Health care organizations must support the security measures that HIPAA specifies for protecting patient privacy. However, an organization can define and use other security measures as long as it reasonably and appropriately supports the standards and specifications for those alternative measures.

VII. Security Practices and Technical Solutions

RHIOs use a variety of security practices and technical solutions to ensure privacy. Few interviewees consider security to be a major planning and implementation challenge, with the possible exceptions of user and entity authentication, and patient and provider identification matching. This may be due partly to the limited scope and relative nascence of several exchanges.

Instead of developing security policies, some RHIOs chose instead to defer to participants' policies and practices. Others drafted policies to which all entities must conform when they exchange data. Clearly, RHIOs must have an overall security policy in place that is separate from participants' policies.

Hospitals supply much of the patient information that emerging RHIOs exchange because they typically are among the first constituents to collect automated data and they often house the largest amount of it. Individual participants tend to shape how a RHIO approaches security; in contrast, privacy policies involve input from a broader array of stakeholders working in concert.

Security Practices

User authentication procedures are necessary to confirm the claimed identity of all users who access data through a RHIO. Authorization procedures are necessary to ensure that appropriate users view the information.

Most interviewees said their RHIOs defer to provider organizations regarding authentication and authorization. As a result, authentication occurs in various ways, some of which are more burdensome than others.

Hospitals typically authenticate their own users and notify the RHIO when physicians and other staff members are credentialed and ready to access RHIO data. Some providers require that other professional staff members vouch for all users through a formal process. At one RHIO, physicians must apply in person at the participating hospital, where they present appropriate identification and submit a written authorization request that includes contact

information and details about their supervisor. After that, the RHIO establishes a user account.

According to most interviewees, authorized persons access their RHIO's system with a unique name and password; some may also use secure token identification. One RHIO is trying to standardize the process so physicians need not enter multiple IDs and passwords to access information through their hospital, their practice, or the exchange.

In general, interviewees did not think that building consensus for and developing these policies was difficult. The real challenges, several of them emphasized, are putting secure authentication and authorization practices in place and getting the resources at both the provider and RHIO levels to make them work. Another challenge, some said, is engaging individual physicians in information exchange and managing the potentially burdensome requirements, such as authentication paperwork and the use of multiple passwords, that doctors must meet to participate in the RHIO.

RHIOs also ensure data security by enabling and tracking the detection of any inappropriate access to or use of data. Most interviewees said their RHIOs can maintain a full audit trail and track several parameters, including user login, the data that have been accessed, and time of access. As a standard security practice, the RHIOs maintain an audit log distinct from the one each participant keeps. Most of these exchanges can match their log with a participant's—when, for example, unauthorized users are suspected—but they do not share their audit information with participants.

Most interviewees indicated that developing and implementing auditing technology and supporting this capability are possible. Concerns and challenges centered on ways to access audit data, the usefulness and clarity of the voluminous reports, and how to inspect the information efficiently.

Another common security practice—frequently referred to as "break the glass"—is to enable data access when authorization fails or emergencies arise. RHIOs in this survey and their participants set different parameters and restrictions on who has authority to gain such access and the situations in which it is acceptable. Typically, override procedures apply in emergencies—for example, when a patient arrives unconscious in the emergency department. Certain designees, such as the emergency department physician or hospital administrators, usually have override authority.

Technical Solutions

It is essential that RHIOs be able to match a patient's and provider's identifications. As RHIOs continue to expand their scope and add patients and providers, the likelihood that two people with the same or similar names will have data in the system is very high. To ensure appropriate data access and use, the RHIOs in this survey have developed processes and protocols to distinguish one "John Smith" from another.

Most of them match patient records through a combination of automated and manual means. The automated process uses specific algorithms that often are the underpinnings of a master patient index.

Some interviewees commented that full automation might not always be accurate. For that reason, several of the RHIOs also use human intervention to ensure 100 percent matching and to eliminate duplicate entries, which can be challenging and labor intensive. For example, issues may arise when a master patient index contains identical names or Social Security numbers.

As the patient population increases, RHIOs must manage the matching process more vigilantly and ensure that protocols for matching are scalable. Several of the exchanges in this survey use a variety of patient protection protocols, such as alerts if patient information is inappropriately sent to a physician or patient records are incorrectly merged.

RHIOs may use both automated and manual processes to match providers, just as they do to match patients. According to several interviewees, this is simpler than matching patients, largely because there are fewer physicians. One noted that a "hole" occurs when a hospital does not inform the RHIO that a physician is no longer affiliated with that facility.

Interviewees suggested that RHIOs link to the human resources systems of participating organizations to more efficiently match physicians, although the RHIOs in this survey do not have that capability. Several said that, as in patient matching, manually removing duplicate entries or physicians who are no longer affiliated with a hospital can be extremely time-consuming.

Distributed vs. Centralized Architecture

For evolving RHIOs, a fundamental decision is selecting an architecture design to support secure data exchange. Their perspective on and concerns about privacy influence this decision.

RHIOs in this study typically use a distributed or a centralized architecture to support information exchange (most chose the former), rather than a combination of the two or a hybrid. In the distributed approach, a network connects separate data systems so the information in them can be exchanged. In the centralized approach, all data reside in one location.

Those who favor a distributed architecture believe that data should reside where they originate but be accessible to all participants. This is consistent with the Markle Foundation's Connecting for Health Common Framework, which "helps information networks…share information among their members and nationwide while protecting privacy and allowing for local autonomy and innovation."[12]

A centralized architecture may be preferable when small participating hospitals do not have the wherewithal to establish comprehensive privacy protections and maintain the necessary infrastructure, and they lack the resources and expertise needed to store data on-site. One RHIO chose the centralized approach because, according to its representative, it believes this model offers stronger protections.

For several of the RHIOs, the setting—particularly one led by an academic medical center (as in Indiana and Memphis) or a vendor (as in Philadelphia)—dictated the type of architecture. In these situations, interviewees said, developing and implementing a security policy around data storage is rarely difficult.

Some of the RHIOs also use secure edge servers, which mirror their internal computer networks but store data outside the main system. This helps them manage the volume of data access requests and any potential impact on the performance of the information systems they need for daily operations.

Technology information protocols ensure that an architecture can encrypt information and exchange it securely. Many RHIOs in this study use a virtual private network and secure sockets layer technology to support such protocols. Some interviewees said that identifying and implementing appropriate protocols is not challenging "if you know what you are doing." Others cited challenges such as connection failures in virtual private networks and getting exchange participants to devote the staff time and dollars necessary to support protocols.

VIII. The Consumer Perspective

Improving patient and consumer services is a major focus of the RHIOs and is at the foundation of their privacy and security policies. Nevertheless, the exchanges are struggling to engage and include consumers in planning and development in a way that will be most effective. With that in mind, the authors took a closer look at the relationship between RHIOs and consumers, the current and potential role of consumers, and the issues ahead.

Collaboration Is Limited

Few RHIOs today seek the advice of consumer experts, patient advocates, or patients as they develop policies, including those related to privacy. Yet experts and some RHIO representatives agree that consumers are key constituents. Collaboration between consumers or advocates and RHIO leaders can help an exchange develop comprehensive and appropriate privacy policies and practices.

There are several reasons why such collaboration is uncommon. They include difficulty in engaging representative or knowledgeable consumers, limited resources to conduct consumer outreach and education, and the fact that many individuals and consumer groups do not understand or believe in the benefits of health information exchange. RHIOs and patient advocates alike are struggling with these issues and considering various countermeasures.

The RHIOs in this report acknowledge the importance and complexity of developing comprehensive and transparent privacy policies, many of which directly affect and concern patients. They address the array of privacy issues very differently and their policies are not always readily available or transparent to consumers. Diverse philosophies about patient rights, control, and choice make it even more difficult to manage these issues.

A patient's right to view and access data can be contentious. While many consumers may expect to have automated access to information about themselves, most RHIOs are not prepared to enable it. One RHIO in this study enables such access by exporting data to the individual's personal health record, but this capability is a longer-term proposition for others.

Some experts and consumer advocates argue that patients should be able to visit their provider electronically and access all of the information about them in the RHIO, not just information the provider houses. Many health care stakeholders agree, but they note that related policies and processes—how patients are authenticated and view data and how to make sure not to overload patients with information, for example—are extremely challenging and beyond the scope of most RHIOs.

Moreover, such access may create more burdens for RHIOs, like the cost of developing the necessary infrastructure and educating patients about data content. (See Appendix A regarding efforts by the American Health Information Community and the Health Information Technology Standards Panel to address these issues.)

The RHIOs in this study use diverse strategies to engage consumers. Some are struggling to identify and engage the most appropriate and representative consumers and to define consumers' roles in information exchange. The North Carolina Health Information and Communications Alliance, Secure Architecture for Exchanging Health Information (SAFEHealth), Michiana, and the Rhode Island Health Information Exchange reach out to and engage consumers differently. But it is still unclear if RHIOs generally want to involve, or can accommodate, educated consumers in planning.

Best Practices and Principles

Patient privacy advocates and some RHIOs believe that addressing privacy issues and potential consumer concerns early in a RHIO's development is crucial. Consumer and privacy experts agree that RHIOs can build on privacy models like the Connecting for Health Common Framework, HIPAA, and others. The Common Framework, in particular, has received much attention; increasingly, RHIOs and other health care stakeholders are referring to this model for recommendations on consumer choice, entity authentication, and architecture for health information exchange.

Consumer-focused best practices are not yet evident in RHIOs. But several organizations, including the Markle Foundation, the National Consumers League, and the Health Privacy Project, have established consumer-directed principles that could serve as best-practice models and guide future RHIO privacy policy.

These principles advise that consumers:

- Know what information about them is in a health information exchange.
- Have access to the information and be able to correct or amend it.
- Understand how the information will be used, who has access to it, and how it can be tracked.
- Control whether and how the information will be shared.
- Be aware of their authority concerning the information, for example, knowing about consent policies.
- Ensure they are notified of breaches in a timely manner and that effective legal remedies are available to them.

As approaches to privacy issues evolve at RHIOs, many consumer advocates would like consumers to play a greater role in developing policies related to privacy and other issues, such as personal health records and pay for performance. Ways to reach out to and engage consumers are emerging. They include consumer councils, consumer-directed focus groups, and consumer and patient representatives on RHIO governing bodies.

Slowly but increasingly, states are collaborating with RHIOs to better understand the priorities and concerns of key health care stakeholders, including consumers. State-based workgroups, for example, give consumers an opportunity to be visible and participate in the dialogue.

There are other barriers to stimulating broader consumer interest in RHIOs. Advocacy groups may not see health information exchange as central to their mission, or they and consumer groups may not see its potential benefits. The tremendous gap in consumer awareness—poor health literacy, for example, and consumers not realizing that complete medication lists and lab results are important—may ultimately hinder exchange efforts.

Organizing workgroups that represent a wide array of interests is one way to communicate with and educate consumers, and to create a broader constituency in favor of health information exchange. Unfortunately, local and national advocacy groups and organizations do not have the financial and human resources to educate all consumers in a coordinated fashion. Perhaps the federal government could support such efforts, as well as forums in which consumers suggest how RHIOs can engage them.

Shortcomings at the Federal Level

The U.S. Government Accountability Office released a report in February 2007, titled "Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy," on how the U.S. Department of Health and Human Services (HHS) is incorporating privacy into its national health information technology strategy.

According to the report, HHS, through its Office of the National Coordinator for Health Information Technology, has spurred efforts to develop solutions for protecting personal health information. But HHS has not come up with a comprehensive plan for integrating those efforts into its strategy and has not set a clear timetable for such integration.

Reconciling state privacy laws, more federal legislation to promote the development and strengthening of local privacy-breach policies, and specifying who is accountable and what the appropriate remedies are when breaches do occur are among other consumer issues that warrant further attention. Some RHIOs face much more restrictive privacy laws than RHIOs in neighboring states do, which suggests that state laws need to be reworked to make them consistent.

There is already movement on this front. Under a contract with the federal Office of the National Coordinator for Health Information Technology, several interests are exploring privacy and security barriers, such as conflicting state laws. These interests include the Confidentiality, Privacy, and Security Workgroup of the American Health Information Community; the Health Information Security and Privacy Collaboration; and RTI International, a research institute. (See Appendix A for more details.)

Interviewees disagreed about whether HIPAA's pre-emption of state privacy laws should be re-examined, but they agreed that HIPAA is only a floor for privacy policy and regulation. The two consumer privacy experts agreed that enforcing the HIPAA Privacy Rule is essential and suggested that the federal government is not doing so effectively.

Patient-consent policies also raise concerns. According to some experts, a RHIO's no-opt policy could prompt a patient to conceal personal health information, not seek care, or seek care elsewhere. Under no-opt, for example, a patient who opposes information exchange and whose physician is unwilling to treat her without complete data may have to find a doctor outside the RHIO. Furthermore, patients who opt out of an exchange, if they have that choice, could limit a hospital's or other provider's ability to deliver high-quality care because potentially critical information would not be accessible.

RHIOs should enlist multiple stakeholders to weigh these issues and design the most appropriate privacy and security policies. Excluding consumers or soliciting their input only after the fact may make the process more challenging and tenuous for everyone involved.

IX. Common Themes

This study revealed a number of themes that could have important implications for the design of privacy and security policies.

Privacy policies and priorities, like health care, are local. Much of what shapes a RHIO's policy depends on local priorities, the types of participants it has, and the level of community trust. The initial focus for most RHIOs is on local data exchange; intrastate and interstate exchanges tend to be a second, third, or even more distant concern.

The institutional perspectives of RHIO organizers influence privacy and security policies. Their background and the "hat they wear"—as a vendor, academician, or clinician, for example—affect their approach to privacy and security issues and their credibility on privacy matters. RHIOs affiliated with academic settings may be more comfortable using data for research purposes, while vendor-led RHIOs may be more technology-oriented in privacy and security matters.

RHIOs should develop privacy policies early and revisit them often. It is more efficient and effective to address privacy policies before the technological infrastructure is designed. Putting this task off until later may result in greater barriers or a revision of technical solutions as these policies expand.

Privacy policies, like RHIOs, are evolutionary. Most exchanges shape them over time based on a RHIO's development stage, priorities, and internal or external pressures to address certain issues quickly.

Work on privacy and security policies is on-going. RHIOs are broadening their goals and scope, adding participants, and exchanging new data. As the types of data and participants increase, so will the number of privacy and security issues. What works today for 500 physicians may not work tomorrow for 5,000, which means RHIOs must adapt their policies over time.

Although few best practices exist, one size will never fit all. Functioning RHIOs and policy models like the Connecting for

Health Common Framework provide some guidance for emerging exchanges, but practices and policies will reflect a community's own priorities and goals. Some variance can be expected and is appropriate.

Building consensus on privacy policies requires time, patience, and resources. This process, which usually has a committee or workgroup driving or informing it, can take months or even years. It requires continuous oversight, review, and the participation of people who have privacy, security, and IT expertise.

Consumers have limited opportunity to influence privacy policy. Hospitals, physicians, privacy and security officers, and IT professionals top the list of constituents who shape privacy and security policy. At only a few RHIOs do consumers formally participate in general or specific policy considerations.

Confidentiality is just a starting point. Nascent RHIOs should anticipate that, in the future, they will need to emphasize the integrity of patient information and ways to secure it.

Education, collaboration, communication, and commitment are critical. A RHIO's success will depend heavily on educating participants (including consumers), collaboration among them, effective and continuous communication, and a commitment to developing comprehensive privacy and security policies. Transparent practices and effective management of privacy and security issues often facilitate and sustain participation in a RHIO because constituents are more knowledgeable and have more confidence in the exchange. RHIOs that designate a privacy champion and a "decisionmaker with authority," and that communicate a strong value proposition, will speed the development of privacy and security policies.

All RHIOs address certain issues. These include selecting a technical solution for secure data exchange, determining patients' role in authorizing data exchange and the extent to which a RHIO should defer to participants' policies, and identifying and matching patient and provider information uniquely.

X. Recommendations

As RHIOs evolve, trust, collaboration, and communication are fundamental to their successful implementation. Successful policies hinge on a RHIO's recognition of the community's sensitivities and priorities. Emerging exchanges must appreciate the local nature of policy questions, quickly start to build consensus around key issues, and, early on, engage a broad cross-section of stakeholders, including consumers, in thoughtful discussion.

Meanwhile, policymakers should further analyze important issues. These include liability concerns, pre-emption of state laws by federal law or resolution of conflicting state laws, consistent and effective consumer remedies for privacy breaches, the implications of patient consent and access to data, and the impact and value of secondary uses of data.

The authors recommend that nascent RHIOs:

Avoid narrow solutions. Strict privacy and security requirements are premature at this point. RHIOs and federal initiatives should use existing models and frameworks only as guides, not as finite or exclusive solutions.

Address external factors. Depending on their near- or mid-term goals, RHIOs can manage privacy and security in various ways. The approaches must be consistent with state and federal laws, with participants' appetite for thinking strategically about the RHIO's growth, and with the community's practices and culture.

Engage a wide range of stakeholders. To maximize possibilities and minimize roadblocks, from the outset RHIOs should consider how to engage all relevant health care stakeholders, including consumers. This will most likely encourage participation in the exchange and expose a range of concerns, even though some may not relate to current or near-term activities or policies.

Look to local privacy and security policies for guidance. Most care providers will already have privacy and security practices and written policies in place. Emerging RHIOs should use these "rules of the road" as a starting point and build upon them. Ultimately, however, they will have to develop policies that still meet local needs.

Refer to HIPAA and state laws at the outset. HIPAA's privacy and security standards are a good starting point. If a RHIO's top priority is to demonstrate a near-term value proposition, it can initially exchange information only among entities covered by HIPAA, and, if more stringent state laws exist, share data only for purposes of treatment, payment, and operations consistent with those laws. This enables a RHIO to proceed without policies beyond those that govern infrastructure operations. For instance, using HIPAA's security standards for audit controls, an exchange can build upon participants' own audit control practices and come to agreement with them on which capabilities the RHIO should maintain and which information should be shared and under what circumstances.

Anticipate long-term infrastructure needs and goals. A RHIO must look beyond its immediate technical capabilities, such as identity mapping, and the system architecture necessary for health information exchange. How will it expand those capabilities down the road? What kind of technical infrastructure and policies will the RHIO need so it can evolve?

Keep sustainability in mind. Thinking ahead, RHIOs should contemplate models that include using data for secondary purposes, such as research or marketing. Because secondary uses are likely to affect the extent of consumer participation, RHIOs should also consider ways to engage consumers more effectively and comfortably in decisions about those uses.

These recommendations are for policymakers and the communities in which RHIOs operate:

Consider future data uses. To meet the long-term goal of sustainability, RHIOs should identify the barriers to secondary uses of data and ways to overcome them.

Share lessons learned. RHIOs should share their experiences with others and explore common solutions or consistent ways to address key issues, such as liability and secondary uses of data.

Pay attention to federal initiatives. It is important to monitor the activities of several federal initiatives, among them the Confidentiality, Privacy, and Security Workgroup of the American Health Information Community, and the Health Information Security and Privacy Collaboration; to learn about new policies; and to give policymakers an "on the ground" versus an insider's view of health information exchange.

Foster discussion. RHIOs and federal and state policymakers should continue to promote forums where interested parties can collaborate, share information, obtain a better understanding of privacy and security issues, and discuss ways to tackle them.

Champion consumer rights. Because consumers' concerns about privacy and security warrant attention, RHIO policy and federal and state laws should address them. In particular, policies and laws should require consumer remedies when security is breached. Consumers will more likely support health information exchange if they trust that it will not compromise the confidentiality and security of their personal data, and that they have redress if a breach occurs.

The RHIOs in this survey have invested significant energy addressing a number of important privacy and security issues. Evidence suggests they are intensely focused on developing related policies in a well-informed, collaborative manner. Although their approaches to privacy and security vary, they can provide valuable insight to other, more nascent exchanges, which can base their initial efforts on one or more of these models and ultimately tailor a solution that meets local needs.

However, most functioning RHIOs acknowledge there is much more privacy and security policy work to be done locally and at the state and federal levels to enable effective, comprehensive, and ultimately widespread health information exchange.

Appendix A: The Federal Privacy and Security Landscape

All federal health agencies have privacy and security responsibilities, and many administrative and congressional activities related to health information technology have privacy and security components. These activities began with HIPAA and continue today through the Office of the National Coordinator for Health Information Technology.

The federal government is primarily concerned about issues requiring national leadership: standards and penalties regarding health information privacy and security standards, information exchange standards, and patient identification. HIPAA includes minimum privacy and security standards, although states may set more-stringent ones.

HIPAA Privacy and Security

Administrative simplification provisions in HIPAA required the U.S. Department of Health and Human Services (HHS) to establish privacy and security rules, national standards for electronic health care transactions, and national identifiers for providers, health plans, and employers. Privacy and security standards went into effect in 2003 and 2005, respectively.

Under HIPAA, providers, plans, and clearinghouses must protect individually identifiable health information. Written consent is required to use or disclose protected health information outside of treatment, payment, or health care operations.

According to HIPAA, entities must analyze the vulnerability of personal health information. Based on that analysis, they must then establish appropriate and reasonable administrative, physical, and technical safeguards to secure the confidentiality, integrity, and accessibility of protected information. The Centers for Medicare & Medicaid Services, the Department of Defense, and the Department of Veterans Affairs also are covered entities and must comply with HIPAA.

Two HHS offices oversee and enforce HIPAA, mostly through voluntary compliance and education. The Office of Civil Rights communicates privacy rights, investigates complaints, and provides extensive guidance (largely to consumers) on HIPAA privacy. The Office of E-Health Standards and Services interprets and enforces the HIPAA Security Rule. Both offices can impose civil monetary penalties for violations. The U.S. Department of Justice investigates possible criminal violations.

The Office of Civil Rights has received more than 20,000 complaints, but it has referred only one case for trial. The Office of E-Health Standards and Services has received few complaints. According to a recent Department of Justice opinion, only covered entities, not their employees, can be prosecuted under HIPAA. In light of this opinion and HIPAA's 2006 enforcement guidelines, which reaffirm HHS's commitment to voluntary compliance, a significant number of HIPAA prosecutions seems unlikely.

Events Since HIPAA

Among the most noteworthy recent events at the federal level are the targeted privacy and security initiatives by the Office of the National Coordinator and the American Health Information Community's creation of a privacy and security workgroup. AHIC is a federal advisory committee with 18 members representing public and private health care stakeholders.

The initiatives include formation of the Health Information Security and Privacy Collaboration, for which RTI International is the contractor. The collaboration will examine best practices and develop solutions for overcoming differences in laws and practices that prevent nationwide data sharing.

The Office of the National Coordinator also has engaged four contractors to create prototype privacy and security architectures for the Nationwide Health Information Network that address privacy and

security issues. The contractors demonstrated their prototypes at the American Health Information Community meeting in January 2007. The Office of the National Coordinator will seek to advance the nationwide network by soliciting contracts in 2007 for trial implementations.

In June 2006, the American Health Information Community announced a new Confidentiality, Privacy, and Security Workgroup that is considering privacy and security issues. However, in February 2007, workgroup co-chair Paul Feldman resigned, citing lack of substantial progress in developing policies to address privacy issues related to health information exchange. Seven workgroups now support the community, whose co-chairs are Michael Leavitt, secretary of HHS, and Dr. David Brailer, former national coordinator for health information technology.

HIPAA assigned another advisory body, the National Committee on Vital Health Statistics, to make privacy and security recommendations to Leavitt. It recommended stronger security measures, possibly to include biometrics, digital signatures, and public key infrastructure, in electronic prescribing and other medical transactions. The committee held hearings on the national patient identifier and issued a report based on them. It continues to weigh in on certain privacy and security standards—for example, by recommending that consumers be given the right to decide if their personal health information will be included in the Nationwide Health Information Network. (The committee was unable to decide if the process should be opt-in or opt-out.)

In November 2006, the committee released a draft report, "Minimum but Inclusive Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network (NHIN)." The report includes guidelines, created at the request of the Office of the National Coordinator, that describe the critical privacy and security elements for connecting to the nationwide network. The committee focused on patient-consent policies, recommending that HHS adopt the following positions:

- Patients should have the right to decide if their personal health information will be included in the nationwide network.
- Providers should not be able to deny treatment to patients who choose not to have their information included.
- Patients should receive culturally sensitive and understandable educational materials about the implications of allowing their personal information to be exchanged.

Chief among the other privacy and security issues in the draft report are authentication, authorization, and matching patients to their information. The committee also recommended that HHS recognize that RHIOs and vendors of personal health records are not necessarily covered entities under HIPAA, and that augmenting or expanding HIPAA might provide equivalent protections for the personal health information that noncovered entities use.

Among other groups operating in the national health privacy and security arena is the Certification Commission for Health Information Technology. It recently certified 55 electronic health record products. The certification criteria include privacy and security specifications. The commission has indicated it may adopt the minimum functional requirements by the National Committee on Vital Statistics as standards for certifying health information exchanges beginning in 2008.

On the Legislative Front

Since HIPAA's privacy and security rules took effect, physicians' slow adoption of health information technology and numerous security failures among government agencies have prompted Congress to consider taking action on privacy and security. The Senate and House passed related bills in the last session.

Senate Bill 1418 contained additional protections for health information privacy. The corresponding House legislation, HR 4157, does not call for changes in federal privacy law nor does the most recent version call for pre-empting state health information security laws, as the original version had initially proposed. HR 5318 was one of several data security bills introduced in Congress after the U.S. Department of Veterans Affairs experienced a pair of security breaches. None of this legislation would be likely to pre-empt state laws governing data breach or notification.

In the new congressional session under Democratic leadership, it is unclear if lawmakers will consider the same bills in 2007. However, Senate Democrats have expressed interest in reviving the legislative push on health information technology issues.

Appendix B: Interviewees

A. John Blair III, M.D.
President and Chief Executive Officer
Taconic IPA Inc.
Taconic Health Information Network and Community

Vicki Estrin
Program Manager, Regional Informatics Programs
Vanderbilt Center for Better Health
Mid-South eHealth Alliance (Memphis RHIO)

Mark Frisse, M.D., M.B.A., M.Sc.
Accenture Professor, Biomedical Informatics
and Director, Regional Informatics Programs
Vanderbilt Center for Better Health
Mid-South eHealth Alliance (Memphis RHIO)

Larry Garber, M.D.
Director, Medical Informatics
Fallon Clinic
Secure Architecture for Exchanging Health
Information (SAFEHealth)

Janlori Goldman
Director, Health Privacy Project
Research Scholar, Center on Medicine as a Profession,
Columbia College of Physicians and Surgeons

Keith Hepp
Chief Financial Officer and
Vice President, Business Development
HealthBridge

Pat Holmstead
Director, Quality Improvement Services
Inland Northwest Health Services
Northwest RHIO

Jay McCutcheon
President, Health Network Services
Health Information Exchange Planning
Implementation and Operations
Michiana Health Information Network

Elliot Menschik, M.D.
Chief Executive Officer
Hx Technologies Inc.
Philadelphia Health Information Exchange

Victoria M. Prescott
General Counsel and Business Development Specialist
Regenstrief Institute Inc.

Peggy Pruesse, R.N.
Privacy Officer
Fallon Clinic
Secure Architecture for Exchanging Health
Information (SAFEHealth)

Robert Reid, M.D.
Director, Medical Affairs
Cottage Health System
Santa Barbara County Care Data Exchange

Allison Rein
Assistant Director, Food and Health Policy
National Consumers League

Mike Skinner
Executive Director
Santa Barbara County Care Data Exchange

Appendix C: Glossary

Note: The use and understanding of privacy and security terms vary. The following are not formal or standard definitions.

Access-rights management

The process of ensuring access rights—that is, who is authorized to see, edit, or remove patient data. Access rights determine which actions users can perform, such as read, write, execute, create, and delete, on shared files in health information exchange.

Centralized architecture

A technology architecture in which all data reside in one location, generally on a central server. It offers security and system management benefits. Disadvantages include concerns about "data ownership" and space for hardware.

Central servers

A hardware configuration that houses data and applications accessible from various points in a computer network.

Decentralized or federated architecture

A network of individual entities that are connected to share data. The information resides, and is maintained locally within individual organizations, but it is accessible via the network.

Edge server

Houses data and applications outside the main computer network of an organization participating in a RHIO.

Master patient index

A computer-based system that links patient information across a variety of health care settings. Due to different name spellings, such as Brown and Browne, and duplicate names, such as more than one John Smith, a master patient index uses a range of data and matching algorithms to ensure that patients are correctly matched to their individual data. An assigned unique identifier facilitates access to patient-specific clinical information at all points of care.

Record-locator service

Provides information about where patient health information is located and where the patient has received care—for example, at a hospital or doctor's office. It does not contain patient data collected at the point of care.

Secure sockets layer

A security protocol methodology designed to create a secure connection to the server for transmitting confidential data via the Internet. It uses public key encryption, one of the industry's strongest encryption methods, to protect data as it travels.

User authorization

The ability to determine which data a user may access and which functions may be performed on them. Authorization is typically based on role. In smaller facilities and physician practices, users sometimes have more than one role because they perform multiple staff functions. An example is a nurse who is both the medical records keeper and receptionist.

User authentication

The ability to verify the identity of a system user. A simple authorization method is to require that the user provide an identifying token and a secret known only to that person. The banking industry uses an ATM card and a PIN to authenticate account holders.

Virtual private network

A way to use a public telecommunication infrastructure, such as the Internet, to give remote offices or individual users secure access to their organization's network.

Endnotes

1. Lassila, K.S. "Assessing the Impact of Community Health Information Networks: A Multi-site Study of the Wisconsin Health Information Network." *Topics in Health Information Management* 1997;18(2): 64–76.
2. McDonald, C.J., Overhage, J.M., Barnes, M., Schadow, G., Blevins, L., Dexter, P.R., Mamlin, B., INPC Management Committee. "The Indiana Network for Patient Care: A Working Local Health Information Infrastructure." *Health Affairs* 2005;24(5): 1214–1220.
3. Starr, P. "Smart Technology, Stunted Policy: Developing Health Information Networks." *Health Affairs* 1997;16(3): 91–105.
4. Brown, E.G. *Regional Health Information Organizations' Modest Start.* Forrester Research. February 2006.
5. For specific examples, see: Agency for Health Research and Quality. *Evolution of State Health Information Exchange: a Study of Vision, Strategy, and Progress.* January 2006.
6. Center for Information Technology Leadership. *The Value of Healthcare Information Exchange and Interoperability (HIEI).* January 2005.
7. Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W., Middleton, B. "The Value of Health Information Exchange and Interoperability." *Health Affairs* 2005 (content.healthaffairs.org/cgi/content/full/hlthaff.w5.10/DC1).
8. Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., Taylor, R. "Can Electronic Medical Records Systems Transform Health Care? Potential Health Benefits, Savings, and Costs." *Health Affairs* 2005;24(5): 1103–1117.
9. Because there is no universal definition of a RHIO or HIE, it is difficult to pinpoint the exact number of initiatives. For estimates, see Brown EG, op. cit.; eHealth Initiative. *Improving the Quality of Healthcare Through Health Information Exchange: Selected Findings from eHealth Initiative's Third Annual Survey of Health Information Exchange Activities at the State, Local and Regional Levels.* September 2006; and Health Information and Management Systems and Society. HIT Dashboard (www.hitdashboard.com/default.aspx).
10. See Note 4, above.
11. Health Information and Management Systems and Society. HIT Dashboard (www.hitdashboard.com/default.aspx).
12. Markle Foundation. *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.* April 2006 (www.connectingforhealth.org/commonframework). The Common Framework, which is publicly available, includes suggested privacy and technical policies, as well as model contract language for business associate agreements with participating entities. Experts in information technology, health privacy law, and policy developed the framework, which Connecting for Health prototype teams in Massachusetts, Indiana, and California have been testing since mid-2005.

CALIFORNIA
HEALTHCARE
FOUNDATION

476 Ninth Street
Oakland, California 94607
Tel: 510.238.1040
Fax: 510.238.1388
www.chcf.org