Service Area Health Information Exchange

A Hospital Data Sharing Community Resource Guide

MARYLAND
HEALTH CARE
COMMISSION

February 2009

COMMISSIONERS

Marilyn Moon, Ph.D., Chair
Vice President and Director, Health Program
American Institutes for Research

Gail R. Wilensky, Ph.D.
Vice Chair
Senior Fellow, Project Hope

Reverend Robert L. Conway
Retired Principal and Teacher
Calvert County Public School System

Garret A. Falcone
Executive Director
Charlestown Retirement Community

Tekedra McGee Jefferson, Esquire
Assistant General Counsel
AOL, LLC

Sharon Krumm, R.N., Ph.D.
Administrator & Director of Nursing
The Sidney Kimmel Cancer Center
Johns Hopkins Hospital

Jeffrey D. Lucht, FSA, MAAA
Aetna Health, Inc.

Barbara Gill McLean, M.A.
Retired, Senior Policy Fellow
University of Maryland School of Medicine

Roscoe M. Moore, Jr., D.V.M., Ph.D., D.Sc.
Retired, U.S. Department of Health
and Human Services

Kurt B. Olsen, Esquire
Klafter and Olsen, LLP

Sylvia Ontaneda-Bernales, Esquire
Ober, Kaler, Grimes & Shriver

Darren W. Petty
Vice President
Maryland State and DC AFL-CIO
General Motors/United Auto Workers

Andrew N. Pollak, M.D.
Associate Professor, Orthopedics
University of MD School of Medicine

Nevins W. Todd, Jr., M.D.
Cardiothoracic and General Surgery
Peninsula Regional Medical Center

Randall P. Worthington
President/Owner
York Insurance Services, Inc.

(Intentionally Left Blank)

Table of Contents

(Intentionally Left Blank)

Preface

Providers interested in exchanging electronic patient information must address challenges related to privacy and security, business practices, technology, and community outreach. Service area health information exchanges (SAHIEs) are beginning to emerge statewide. SAHIEs are typically made up of providers in a select geographic area that share the same patients across practices and settings. In an effort to increase efficiency and quality of care, providers have begun to collaborate on ways to share patient information electronically. Chief information officers, privacy officers and various other health care stakeholders participated in a workgroup to develop a resource guide that would include a core set of policies to guide SAHIEs in their planning efforts. Workgroup participants agreed that the exchange of patient information carries with it great responsibility and adherence to a stringent set of standards that generally exceed most other technology adoption projects. This resource guide is a reflection of their commitment to ensure that communities that embark on data sharing implement similar policies.

The workgroup unanimously agreed on a guiding principle that patients should control the flow of information through an exchange, and safeguards must be put in place to govern disclosure and assure proper authorization for data access. Patients are likely to have questions regarding the exchange of their health information and SAHIEs will need to be prepared to address these concerns when they arise. Requests for patient amendment of records carry additional challenges when multiple data sources are included. The Health Insurance Portability and Accountability Act of 1996, (HIPAA), Administrative Simplification provisions provide guidance around privacy and security. Workgroup participants chose to develop policies that exceeded HIPAA and would likely build consumer trust.

Providers must resolve a number of business practice considerations in designing and building a SAHIE. The workgroup focused on business practices that center around access, authentication, authorization, and audit. Workgroup participants decided to address these business practices from the perspective of the provider and the consumer. While technology is usually not the most challenging aspect of a SAHIE effort, it is critical that certain standards are adopted to ensure interoperability. The workgroup also addressed hardware, software, encryption, and networking requirements.

One of the key early steps in SAHIE development is the identification and engagement of the stakeholders. The workgroup noted that participants in a SAHIE effort often have divergent business interests; identifying common ground early in the process is a key success factor. SAHIEs must also establish a community roadmap, so all participants are clear of what the initiative entails both initially and as the exchange expands. Determining the amount and level of communications concerning SAHIE efforts requires accounting for differences in social, economic, and cultural variances within each community.

Identifying an appropriate funding mechanism for SAHIEs remains a challenge for most communities. The workgroup agreed that SAHIEs should explore opportunities to take advantage of the relaxed Stark regulations and the benefit of Safe Harbor provisions in contracting. SAHIEs will need to consider different funding models in order to identify a system where participants are appropriately assessed a fee based upon value. Resolving issues relating to funding are a significant challenge; by following a valuation process to the participant’s reasonable funding mechanisms can be identified.

Alternate data use presents policy challenges for SAHIEs as they contemplate the appropriateness of using patient data for purposes other than direct patient care. The workgroup agreed that data usages outside the normal parameters of treatment, payment, and operations should be transparent to all users and expressly permitted by the patients. In addition to standard consent processes, the use of secondary data will likely require a public awareness campaign in order for consumers to gain trust in the use of their information. The most common secondary useage for data by SAHIEs include public health reporting, bio-surveillance, and academic research.

Report Limitations

This resource guide represents the views of the workgroup participants and is intended to serve as a tool for providers that are planning to exchange patient information electronically. Information contained in this resource guide is aimed at providing users with key policy information related to areas where the workgroup felt that consistent policies across SAHIEs is essential to the broader goal of statewide data sharing. Users of the resource guide are encouraged to consider adopting the recommended policies and to fully consider the impact of these recommendations on their organization before implementing.

Acknowledgements

Maryland Health Care Commission (MHCC) thanks the more than thirty workgroup participants from hospitals and other stakeholder groups for their commitment of time and expertise in the development of this resource guide. The level of cooperation among workgroup participants, and their willingness to share ideas and engage in healthy debate is a reflection of the level of interest for harmonizing efforts to connect service area providers, which many view as an important first step toward data sharing across communities. MHCC appreciates the assistance it received on this initiative from Dynamed Solutions and Audacious Inquiry.

Service Area Health Information Exchange

Background

Exchanging clinical data within service areas establishes a foundation for connecting communities through a statewide health information exchange. Enabling treating providers to share health information about a patient improves the overall safety, effectiveness, and efficiency of health care delivery. Collaboration among providers on technology and privacy and security policy plays a critical role in communities to effectively share vital patient information. Developing sound policy pertaining to privacy and security that is agreed upon within service area health information exchanges (SAHIEs) is an essential first step in connecting providers. The Maryland Health Care Commission (MHCC) convened a workgroup at the request of health care stakeholders to develop a resource guide containing privacy and security policy and technology guidance for providers in the planning stages of a SAHIE.

Hospitals typically serve as the convener of a SAHIE initiative as they have the technical resources, established connections to the provider community and other essential stakeholders, and possess much of the data that is required in care delivery. In 2008, MHCC conducted a health information technology assessment of Maryland hospitals.[1] Findings from the assessment indicated that few SAHIEs exist formally and that most of them are exchanging some patient information electronically. Nearly all hospitals indicated that they are evaluating data sharing opportunities.[2] Information contained in this resource guide is intended to assist providers that are planning to share electronic patient information with guidance as they move forward with implementing a SAHIE.

[1] Health Information Technology Adoption Survey developed by the MHCC to measure adoption and implementation of health IT among the State's 47 acute care hospitals.

[2] The SAHIE Environmental Scan Results presentation is located on MHCC's website at: http://mhcc.maryland.gov/electronichealth/SAHIESURVEYRESULTS-7-8-08-FINAL.pdf.

Patient Rights to Their Electronic Health Information

Patient rights to their medical records is governed under the Maryland Confidentiality of Medical Records Act (MCMRA)[3] and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.[4] In general, both MCMRA and HIPAA state that individuals have the right to view, get a copy of, and request amendment of records for themselves; dependent, unmarried children under the age of eighteen; and individuals for whom they have the right to make medical decisions, such as under an advance directive. In these cases, rights extend only to those records associated with the specific treatment for which they are making decisions, and not to older, non-relevant records.

The workgroup agreed that providing patients with control over the flow of their health information is necessary to foster transparency within the exchange and instrumental to building trust among stakeholders. Determining the control patients have regarding who accesses their data, the patients' rights for authorizing disclosure, the accounting of disclosure to the patient, and the patients' rights to amend or note discrepancies in their medical record needs a standardized approach among SAHIEs. The workgroup used the Connecting for Health Common Framework for Networked Personal Health Information as a guide in developing their recommendations. This document provides a foundation for building trust among all participants and supports patient control over their health information.[5]

[3] Maryland Code, Health General. §4–301 et seq. (1991).

[4] For a full consideration of the differences between operative Maryland and federal law, by category and cross section, see http://www.dhmh.state.md.us/sacmpc/pdf/compchart.pdf.

[5] Markle Foundation, *Connecting for Health: Common Framework for Networked Personal Health Information*, 2008. Available online at: http://www.connectingforhealth.org/phti/reports/cp8.html.

Patient Should Control the Flow of Their Electronic Health Information

Issue

In the current paper environment, patients have the ability to control what information is disclosed to any provider, including information regarding other treating providers. Patients should also be able to control who has access to their electronic health information. The workgroup agreed that the patient's ability under most circumstances to selectively share information is appropriate for exchanging electronic patient information. SAHIEs will need to consider the extent of patient control so that this control does not impede one's treatment or well being. Patients should be able to grant permission to specific treating providers with consideration for more stringent patient control over their sensitive health information, which includes mental health, substance abuse, and sexual history.[6]

Key Decisions

- Develop a mechanism for physicians to register with the data sharing entity
- Identify a process for patients to grant authorization to treating providers
- Establish a process for patients to control what information an authorized person, provider, or entity can access
- Develop a process for patients to control access to sensitive health information
- Establish a method for patients to rescind authorization previously granted

Discussion

A core set of data should be available when patients seek and initiate care, and patients must be educated to the importance of designating access controls of their information to their treating providers. Workgroup participants felt that SAHIEs should include in the data exchange a notation to providers of what categories of information are withheld from the record they are reviewing. SAHIEs must consider patient education as a key activity to ensure that patients have a clear understanding of the data elements they will be able to control and those they may not, and the reasoning behind these decisions.

[6] William A. Yasnoff presentation, *A New Patient-Centric and Sustainable RHIO Model*, Scottsdale Institute Teleconference, October 3, 2005.

Patient Must Have Right to Request Amendment to Electronic Health Information

Issue

Patients currently have the right to request amendments to their health information. The conventional paper system in place today makes it difficult for patients to have easy access to this information. Patients will have a more systematic and structured way to view their health information in an electronic environment. Information regarding the source, or originator, of the data should be available to the patient in the event that the patient has questions, concerns, or chooses to request an amendment to the information contained in their electronic health record. The workgroup believed establishing policies that allow patients to amend their health information is necessary to ensure that data sharing remains patient centered.

Key Decisions

- Implement a process for patients to inquire about incomplete, missing, or inaccurate information
- Establish a method to identify the originator of data stored or transmitted
- Develop a process to provide consumers with select information from an electronic data set
- Identify a method to disseminate amended data to providers that have accessed consumer information
- Establish a process to remove incorrect information from an electronic data set
- Identify a method to include requests, either granted or denied, in a consumer's electronic health record
- Implement a plan for notifying patients of an amendment decision per the receipt of a written request
- Establish a process for moderating unresolved data amendment requests

Discussion

The workgroup agreed that patients should have the right to request an amendment to their electronic health record. Ideally, these requests should be submitted to the originating provider, and providers should deny amendment requests if they believe current records are accurate and complete, or if they did not create the information. Patient rebuttals and/or denials to amend information should become part of the patient's electronic health record. Robust data sharing may complicate identifying the original source of a patient's data as providers may include particular elements of a requested patient record into their own records. SAHIEs will need to ensure that any known holder of the information is informed of the amendment.[7]

[7] Ibid.

Patient Must Be Informed of Disclosure of Electronic Protected Health Information

Issue

The disclosure of health information is necessary for the delivery of high quality health care. The workgroup felt that sharing information for patient care is essential, and that providers should notify patients in advance of the potential for sharing electronic patient information with other providers. Disclosure of health information for the purposes of treatment, payment, and operations is permitted under the HIPAA privacy rule.[8] However, the workgroup felt that advance notification to patients will increase patient confidence in the sharing of their electronic health information.

Key Decisions

- Implement a procedure to obtain patient authorization to share health information electronically
- Establish a process to limit routine disclosure of data to providers in accordance with HIPAA
- Establish a process to identify those individuals who are accessing electronic consumer information
- Establish system audit logs of information accessed electronically
- Implement a process for consumers to request who has accessed their electronic data

Discussion

The workgroup felt that HIPAA only serves as a baseline for disclosure of electronic health information and agreed that more stringent policies are required. A primary goal of HIPAA was to encourage electronic transactions among health care plans and providers, while keeping patients' health information private. Based on the experiences from other industries, where confidential information often has fallen prey to computer hackers, the workgroup expressed concerns that the law's protections may not be satisfactory. A well coordinated effort among all providers to educate patients on the disclosure of health information will help ensure patients understand the value of data sharing within communities. SAHIEs will need to routinely track uses and disclosures of protected health information.

[8] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Administrative Simplification Regulation Text, 45 CFR Parts 160, 162, and 164.

Disclosure of Protected Health Information to Surrogates

Issue

SAHIEs should allow surrogate access to pertinent electronic health information. The workgroup agreed that SAHIEs should accommodate proxy access to a patient's health information. A SAHIE that has been informed of a surrogate's request to access patient information should make available an appropriate provider to review the information, explain matters, and answer questions. In short, this is an opportunity for SAHIE providers to bolster communication with the surrogate. Proxy access should be managed through a separate login and authentication process. Patients should be able to set surrogate access levels around viewing data.

Key Decisions

- Establish a process for authorizing surrogates to access electronic health information
- Identify a process for disclosing data to appropriately authorized surrogates
- Establish levels of surrogate access to electronic health information
- Develop a method to audit surrogate activity of an electronic data set
- Implement a process to rescind surrogate designation and access to a consumer's electronic data

Discussion

Consumers need a process to permit surrogate access to electronic information that is required for a surrogate to make decisions about the patient. Surrogates provide a valuable service to patients in need of assistance and often are faced with making difficult decisions.[9] SAHIEs must navigate surrogate decision-makers through a difficult course of treatment decisions and such a process can be complex. The SAHIE must make medical facts and prognoses available to the authorized surrogate to ensure that the surrogate arrives at decisions that are consistent with the patient's own values and wishes. The workgroup felt that SAHIEs have a duty to ensure that surrogates have complete and accurate information on which to base their decisions. SAHIEs will need to establish policies to manage surrogate access and provide guidance to both patients and surrogates in regards to managing access to the data.

[9] Department of Health and Human Services, Office of Civil Rights, *HIPAA Privacy-Personal Representatives.* Available online at: http://www.hhs.gov/ocr/privacy/hipaa/faq/personal/.

Range of Business Practices

Variation in business practices exists across provider organizations and often reflects differences in technology and operations. The manner in which providers implement required security and privacy policies varies and is tailored to meet their individual organization's needs.[10] These variations in policies present challenges for widespread electronic health information exchange. The lack of experience within organizations designed to govern data sharing, and the uncertainty about how to move forward in a responsible manner, has major implications for SAHIEs seeking to design and put into practice privacy and security solutions. Establishing common business practices among providers is essential for exchanging patient information electronically.

Several critical recommendations emerged from the workgroup as it relates to access, authentication, authorization, and audit. Workgroup participants chose to address each area from the perspective of the provider and the consumer. By focusing on common policies regarding these key business practices, SAHIEs will be better aligned for participating in a statewide health information exchange. The approach to access, authentication, authorization, and audit will vary slightly between SAHIEs. Each SAHIE will need to identify appropriate policies that include the different perspectives of those that share the same information.

[10] Information Society Technologies, *A Roadmap for Interoperability of eHealth Systems in Support of COM 356 with Special Emphasis on Semantic Interoperability*, June 15, 2006. Available online at: http://www.srdc.metu.edu.tr/webpage/projects/ride/deliverables/RIDED%202%201%201%20-%20CurrentPracticesUS.doc.

Access

Issue

Defining access to data is critical to ensuring the information is appropriately used and safeguarded.[11] To prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of the information, SAHIEs will need to establish appropriate physical and managerial procedures to safeguard the information that is exchanged. The workgroup felt that SAHIEs need to harmonize access requirements across related users and agree on suitable access levels. User identities must be associated with a role that defines an appropriate level of access to electronic health information.

Key Decisions

Providers

- Establish centralized role definitions consistent with participant's job responsibility and need for access to health information
- Develop role definitions to be adopted by all participants and measures to ensure that adherence to the guidelines for assigning these roles are followed
- Implement robust initial training and on-going provider training programs

Consumers

- Develop a process to grant consumers system access
- Identify a data set that consumers can access (e.g., medications, allergies, diagnosis, lab/radiology results) and data that patients cannot access (e.g., provider notes for mental health and substance abuse)
- Establish a process for providers to release select information for consumer access through a secure web application
- Establish a process to terminate consumer access to electronic data

Discussion

One of the challenges that SAHIEs face is making electronic health information secure but allow reasonable speedy access to providers and consumers. The workgroup felt that role-based access offers the greatest protections to the privacy and security of electronic health information. As the clinical value of accessibility to greater amounts of health information increases, so does the risk associated with managing access and ensuring appropriate usage. This is very different from the paper-based system that exists today where staff frequently has physical access to more information than is minimally necessary. SAHIEs will need to identify the elements of a patient's record that belongs in a shared dataset and carefully define the policies around establishing permissions to the data.

[11] Sun Microsystems, *Implementing Health Information Technology for RHIO Success*, September 2005. Available online at: http://www.sun.com/software/whitepapers/integration_suite/rhio_healthercare_wp.pdf.

Authentication

Issue

Managing authentication depends largely upon the level of integration between the SAHIE and participants. The workgroup felt that either a web application or a centralized approach would provide SAHIEs with an adequate way to manage authentication. Authentication services naturally exist centrally in a client or web-based access model,[12] and exist within the client application in a non-integrated client model because the application is deployed at the participating entity's site.

Key Decisions

Providers

- Identify authentication standards for a strong password and username scheme for participants logging into and accessing electronic data
- Develop a process to ensure that participants are adhering to authentication standards and that IDs and passwords meet strong authentication standards
- Identify a process to limit the number of system login failures to three
- Establish a method to notify users of system login failures with their user ID
- Identify a process to re-establish users to the system when their ID has been locked out

Consumers

- Identify authentication standards for a strong password and username scheme for consumers logging into and accessing data
- Develop a process to ensure that consumers are adhering to authentication standards and that IDs and passwords meet strong authentication standards
- Identify a process to limit the number of system login failures to three
- Develop a process to notify users of system login failures with their user ID
- Identify a process to re-establish users to the system when their ID has been locked out

Discussion

SAHIEs need to determine an appropriate balance between usability and security. Workgroup participants agreed that if authentication requirements are too onerous, then the SAHIE could face adoption challenges and acceptance issues by participants and consumers. Conversely, if the requirements are too relaxed the exchange will compromise data security and suffer from system breaches, or the inherent lack of trust in an unsecure environment. Either of these outcomes would be detrimental to the near-term viability of the exchange. SAHIEs will need to agree on a core set of authentication policies that participating organizations will trust and consumers will accept.

[12] In a non-integrated client application deployed at the participating entities site, authentication services could exist within that client application.

Authorization

Issue

SAHIEs need to place emphasis on securing data that is shared electronically with providers. Data sharing challenges related to protecting patient information has placed additional challenges forcing extra levels of security to allow appropriate individuals to use the data. The workgroup believed that participating organizations need to establish stringent guidelines around the functions that authorized users are able to perform. The guidelines must take into consideration precautions that address users once they have been identified, proven that they are indeed who they claim to be, and provided access based upon the appropriate role. The SAHIE must then verify the functions the user is authorized to perform.[13] These functions could be as simple as distinguishing between the ability to view data, view and contribute data, or the ability to see specific types of data.

Key Decisions

Providers

- Develop an incremental approach to authorization levels:
  - Near-term - allow authorized users access to a set of critical clinical data such as medications, allergies, and current and past medical conditions
  - Mid-term - allow sensitivities to be associated to data, then base authorization levels on the sensitivities
  - Long term - pursue more sophisticated authorization schemes; for instance, functions could include read only, read and write with restrictions depending on authorization level, or full access read, write, and download clinical data
- Implement authorization levels consistent with the user's access role

Consumers

- Develop a process to allow patients the ability to view their electronic health information
- Establish a method for patients to annotate, but not edit, their electronic data
- Identify a process for patients to contribute information to their electronic data set
- Establish parameters to limit a patient's authorization to provider and clinical notes

Discussion

A sound infrastructure that adequately addresses authorization is essential in order to determine the information that users are accessing and perform only the functions for which they are authorized. The workgroup felt that determining the structure mostly depends on the appropriate balance between the complexity, usability, and administrative complexity of each provider community. SAHIEs should develop an incremental approach for authorization that assesses near-term capabilities and long-term goals to ensure that patient safety and quality of care are not sacrificed.

[13] Markle Foundation, *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, 2006. Available online at: http://www.connectingforhealth.org/commonframework/.

Audit

Issue

In concert with organizational confidentiality and security policies and procedures, audit trails can clearly identify all system application users who have accessed the system, record the nature of the information accessed, and maintain a permanent record of the actions taken by the user.[14] Effective audit practices are essential safeguards as electronic health information is shared. Auditing monitors user activities to ensure that all activities within the exchange are performed by authorized users. The workgroup agreed that auditing can build user confidence that other participants are in compliance with defined requirements for technical, physical, and administrative safeguards. SAHIEs that implement a defined method to monitor and review who has accessed patient data generally have more effective security oversight as compared to traditional paper record environments.

Key Decisions

Providers

- Develop written guidelines that detail the frequency and amount of information that is routinely audited
- Identify a centralized auditing mechanism that ensures data shared electronically is appropriately monitored
- Identify a method to manually review subsets of the audit logs created through transaction recording
- Establish audit event rules that identify and escalate certain events to manual review
- Develop measures to ensure data sharing participants are adhering to the audit protocols
- Establish a process to investigate breaches and complaints that provide for reasonable and timely resolution
- Implement a specific audit review of VIP and sensitive data sets

Consumers

- Develop a process that allows data sharing participants to record all access and activity through a consumer access solution application
- Identify a procedure that escalates automatic system audit logs review to a manual review when activity exceeds or varies from defined thresholds
- Establish a process to ensure that consumer access audit practices are clearly communicated to consumers

Discussion

Auditing within a SAHIE, whether for provider access or consumer access, serves to provide a backstop against inappropriate usage. Having the ability to monitor access and activity can provide the necessary safeguards a SAHIE will require to protect the data and foster an environment built on trust. The workgroup agreed that SAHIEs need to conduct robust discussions up-front about the need for audit capabilities, while recognizing that such capabilities may not be implemented immediately. SAHIEs will need to establish and maintain appropriate oversight of key areas that impact access, authentication, and authorization; and include reviewable standards for technical, physical, and administrative safeguards.

[14] Care Evolution Healthcare Technology, *Security & Privacy Mandates for RHIO Architectures, A candid discussion of the RHIO security and privacy needs vis-à-vis current technology option*. Available online at: http://www.careevolution.com/SecurityAndPrivacy.pdf.

Technical Requirements

A number of initiatives in both the government and private sector are currently underway to define the technical requirements for electronic health information. Among the most prominent are the work of the American Health Information Community, which is a federally chartered advisory board that is coordinating the development of national data sharing standards; the Certification Commission for Health Information Technology, a private sector organization focused on certifying electronic health records; and the Health Information Technology Standards Panel that is bringing together stakeholders to agree on interoperability standards. Where possible, the workgroup has formulated its recommendations to comply with standards and policies developed by these organizations. SAHIEs will need to decide on the standards and versioning of the standards in order to minimize participant connectivity challenges.[15]

The technical requirements to data sharing are mostly due to incompatibility in hardware, software, and data file structures. In early computer technology, technical factors sometimes constituted nearly insurmountable challenges to transferring data from one computer to another. Presently, difficulties in data sharing are largely due to the practices and processes rather than technical factors. Provider communities planning to share electronic patient information should carefully evaluate standards, software, and hardware challenges for the different types of participants and their sophistication with technology. SAHIEs should complete a technology assessment early in the process to determine system modifications, additional technology, and costs associated with data sharing.

[15] J. Mark Overhage, Health Information Exchange: 'Lex Parsimoniae,' *Health Affairs, 26*(5), w595-w597, 2007.

Technical Standards

Issue

Technical standards focus on the physical transmission and receipt of information, which can provide guidance and a basic level of security for sharing data electronically. The workgroup agreed that technical standards are in a continual state of development and change. Consideration should be given to the fact that implementing very specific requirements may impede data sharing as they are rapidly outdated with technical advances. The deployment and use of technology that were built on proprietary standards and different versions within standards has created a technical environment where harmonizing efforts often require intensive time, workforce, and financial resource commitments. SAHIEs will need to implement technology that supports communications across varied technologies to ensure inclusion of the participants.[16]

Key Decisions

Message Formats

- Implement DICOM – a standard for handling, storing, printing, and transmitting information in medical imaging
- Develop a process to evaluate and select a version of HL7 – a message standard supporting clinical data exchange
- Implement data sharing profiles from IHE – a technical framework that defines integration profiles to serve as an implementation guide
- Adopt the electronic data exchange standards of X12 – an electronic standard setting committee widely used for integrating electronic applications
- Implement NCPDP – the transactions used for transmitting prescription information

Message Transport Protocols

- Exchange information through a distributed environment using SOAP – a protocol which controls a transport layer with HTTP or SMTP for exchanging XML-based messages over computer networks
- Implement ebXML to support advanced information sharing – a derivative of the XML that enables the global use of electronic business information in an interoperable, secure, and consistent manner
- Implement SSL and TSL – cryptographic protocols that provide secure communications over the Internet

Discussion

SAHIEs need to find the right balance to avoid implementing too stringent technical standards that may negatively impact on the extremely heterogeneous nature of the provider community. Implementing technical standards into a data sharing environment that have been endorsed by a standard setting body ensures SAHIE participants that they can exchange data with and use data from other systems. Technical standards are the foundation for sharing patient information electronically. Absent agreed upon data sharing standards, consumer information will remain locked in provider technology silos, and unable to follow consumers as they obtain care from other providers. SAHIEs need to adopt standards that enable provider systems to communicate to manage and use electronic patient information. The workgroup agreed that SAHIEs must not rely on protocols that are proprietary in nature and that they must resolve critical environmental heterogeneity challenges.

[16] Foundation of Research and Education of AHIMA, The State-Level Health Information Exchange Consensus Project HIE Policies and Practices, *Developing Options and Implementation Guidance To Foster Consistency,* Interim Report Version 1.0, August 15, 2008. Available online at: http://www.slhie.org/Docs/HIEPoliciesandPractices.pdf.

Improve Process Workflows

Issue

Implementing a SAHIE requires participants to address issues relating to change management beyond technology adoption.[17] Challenges include restructuring workflows, dealing with user resistance, and creating a collaborative environment that fosters communication. Most of the existing clinical paper processes should be converged, streamlined, assimilated, and optimized during the redesign process. The workgroup felt that leading barriers to technology adoption can be minimized when project managers carefully consider how existing clinical workflows need to change in order to best utilize technology. SAHIEs should start by gaining an understanding as to how shared clinical data supports the specific activities and workflow of providers that use the data, as well as its integration into the work environment.

Key Decisions

- Develop a process to assess and document current clinical and procedural workflows
- Evaluate where electronic data should be injected into the clinical setting and develop a plan for integrating existing and new workflows efficiently
- Develop an evaluation process to consider any new human resource skills required to realize the full benefit of data sharing
- Deploy training resources (both delivery and content) necessary to effectively support exchanging data electronically
- Identify infrastructure requirements to support data sharing
- Establish a process to assess workflow interdependencies and interrelationships

Discussion

Enhancing workflows should be a continued focus for SAHIEs, all in an effort to achieve operational efficiencies in an electronic environment. The workgroup agreed that data sharing providers should carefully evaluate existing processes, select appropriate processes for redesign, and then execute necessary changes in workflows. A detailed analysis of existing workflows needs to be completed to determine the impact of a mostly paper process on the critical success factors for data sharing.[18] A well-structured process management analysis will help identify workflows of a paper-based office that needs to be restructured to create a more agile and efficient electronic environment. Workflow redesign is an essential component of data sharing as technology alone will not ensure that the benefits are realized.

[17] Alec Sharp and Patrick McDermott, *Workflow Modeling – Tools for Process Improvement and Application Development,* Massachusetts: Artech House Inc.; 2001.

[18] Joseph A. De Feo and William W. Barnard, *Juran Institute's Six Sigma Breakthrough and Beyond: Quality Performance Breakthrough Methods,* New York: McGraw-Hill; 2005.

Communication Mechanisms and Outreach Initiatives

Data sharing must meet the needs of a variety of stakeholders and be secure, protect confidentiality, and make information easily accessible by the appropriate parties. SAHIEs need to take a proactive approach to involving the community in an effort to address questions and understand their concerns. Lack of sufficient community support hinders data sharing initiatives as many of the supporters are essentially data providers, data users, and data funders.[19] Communities that have made strides in implementing data sharing initiatives generally report strong ties with the community.[20] Facilitating community involvement in the SAHIE, establishing communication mechanisms, and developing outreach initiatives are essential to successful data sharing.

SAHIEs need to develop a strategic communications plan designed for process transparency that can mitigate the impact of impediments that could weaken community support and threaten forward momentum. An effective strategic communications plan should leverage existing areas of consensus and establish a structure for communicating progress and resolving the conflicts that are sure to arise. The strategy must be fluid in order to accommodate future elements that can impact community support. Included in the communication plan should be a defined structure and direction for regular dissemination of information and open, ongoing communication to maintain that transparency. Absent a sound plan, the path to long term sustainability is questionable and filled with former supporters who, frustrated by a lack of information or sense of the initiative’s accomplishments, have disengaged from the data sharing initiative.

[19] Joy M. Grossman, Kathryn L. Kushner, and Elizabeth A. November, *Creating Sustainable Local Health Information Exchanges: Can Barriers to Stakeholder Participation be Overcome?*, Center for Studying Health System Change and National Institute for Health Care Management Foundation, no. 2, February 2008. Available online at: http://www.hschange.com/CONTENT/970/970.pdf.

[20] The Agency for Healthcare Research and Quality, *Evolution of State Health Information Exchange: A Study of Vision, Strategy, and Progress*, January 2006. Available online at: http://www.avalerehealth.net/research/docs/State_based_Health_Information_Exchange_Final_Report.pdf.

Secure Stakeholder Engagement

Issue

Communities embarking on a data sharing initiative require appropriate stakeholder involvement during the planning and implementation stage.[21] Transparency from the very beginning of the initiative is critical to retaining community support. The workgroup felt the best way to achieve transparency is to centralize information, then build active communication channels to disseminate information to the stakeholders. A well-developed communication plan should serve as a roadmap for informing stakeholders. SAHIEs need to shape public opinion early in the planning stages in order to establish a sound framework where consumers and providers trust that electronic data will be used appropriately and adequately safeguarded. One of the key challenges in developing a communication and outreach plan is to adequately address the often competing interests of the stakeholders.

Key Decisions

- Develop a communication strategy to raise stakeholder awareness on the purpose and benefits of data sharing that targets everyone in the community
- Identify key individual stakeholders that can serve as champions for data sharing
- Develop a process to track and disseminate information to the community about select consumer success stories pertaining to community data sharing
- Identify critical activities required for a community to build transparency from the very beginning that details a timeline for implementing each of the data sharing services

Discussion

Stakeholder participation helps to build support on potentially controversial issues and establishes a base of information and opinions from which SAHIEs can draw when it comes time to make critical decisions that may affect the future of data sharing. By introducing necessary discussion items through various communication channels, valuable input can be gathered for later use. The workgroup emphasized that SAHIEs should develop a plan that addresses key communication requirements to ensure that stakeholders are engaged but not overburdened. Data sharing initiatives will benefit from erring on the side of stakeholder inclusiveness, so that all views are expressed and considered when developing and implementing a SAHIE.

[21] Pennsylvania eHealth Initiative, *Annual Report: Pennsylvania eHealth Initiative*, December 2006. Available online at: http://www.paehi.org/Documents/PAeHI%20Annual%20Report.pdf.

Define the Message

Issue

Establishing a set of clearly defined common goals that achieve the shared community vision and purpose of data sharing necessitates opening a dialogue across stakeholders to acquire consensus on a variety of complex issues. SAHIEs need to help stakeholders define core principles they all truly share in their quest to share data.[22] Identifying a value proposition that explains the benefits of participation that are unique to their community is also an effective communication strategy. The workgroup agreed that developing a robust message that addresses data sharing is essential to sustainability, and that the benefits of data sharing can be lost among privacy and security concerns. It is important that SAHIEs identify a value proposition in order to transform stakeholder uncertainty into collaboration.

Key Decisions

- Develop a process to build awareness and understanding of the benefits for data sharing unique to each community
- Form a distinct message customized for different segments of the population that underscores value, trust, and maintaining privacy and security of electronic health information
- Establish a process for disseminating key information designed to meet the specific needs of a particular audience that is aimed at building awareness levels about community data sharing
- Develop a plan to leverage existing trust relationships between consumers and providers as a way to reinforce any message that is developed for each segment of the population within the community

Discussion

SAHIEs should facilitate an ongoing dialogue among stakeholders to ensure that the interests and perspectives of all stakeholder groups are addressed as a whole. The workgroup felt that a well articulated message will enhance both consumer and participant support for data sharing. SAHIEs need to be proactive in their effort to disseminate information and include actual events that convey the human experiences. Leveraging the demonstrated value of the SAHIE in the communication process will increase community support and encourage participation. The workgroup viewed outreach activities as a key requirement for sustainability and felt that the more SAHIEs do to demonstrate value the more likely stakeholders will support data sharing.

[22] Selena Chavis, Hardly Elementary: Creating a Successful RHIO, *For the Record*, 19*(3)*: 12. Available online at: http://www.fortherecordmag.com/archives/ftr_06252007p12.shtml.

Anticipate Ethical, Social, and Economic Communication Issues

Issue

Transcending community diversity and building acceptance for electronic clinical information requires an ongoing discussion among stakeholders regarding values and expectations.[23] SAHIEs should assess the benefits and challenges of the cultural and socio-economic differences of the community. Cultural and socio-economic differences often affect how health care is delivered, received, and perceived. The workgroup felt that SAHIEs must be sensitive to the distribution of the population and recognize that variations exist in the way each population expects to receive care. Resolving these variations presents a huge challenge for SAHIEs and can make the difference in the way communities view data sharing. Outreach initiatives need to be customized to meet the needs of the populations that exist in each community.

Key Decisions

- Develop a vision for data sharing that engages diverse stakeholders
- Identify variation in community demographics
- Determine the most beneficial data sharing services for the community
- Develop a process to create transparency by using the Internet to make information easily accessible to stakeholders
- Develop various outreach programs in consultation with representatives from disadvantaged populations
- Implement a communication plan that takes advantage of diverse mediums through which information can be communicated to diverse consumers

Discussion

SAHIEs need to be sensitive to the different populations that exist in each community. Engaging stakeholders that represent different populations is necessary to maximize the value of data sharing for each community. Change management strategies are essential to address the cultural resistance inherent to moving from a paper to an electronic environment. Some initial resistance to data sharing is likely to occur as a cultural shift in favor of electronic information requires time; the length of time depends largely on the communication strategy.[24] Outreach and communication initiatives should be developed that takes into account the variation that exists within each community. The workgroup cautioned against allowing the fundamental challenges of data sharing to deter SAHIEs from addressing the challenges of diverse populations.

[23] Leigh Burchell, ed., *Best Practices for Community Health Information Exchange*, Center For Community Health Leadership. Available online at: http://gd2b.pro-faces.com/files/misys_bestpractices.pdf.

[24] U.S. Department of Health and Human Services, Office of the National Coordinator for Health IT, *Report From The Health Information Communication And Data Exchange Taskforce To The State Alliance For E-Health*, October 3, 2007. Available online at: http://www.nga.org/Files/pdf/0710EHEALTHHICDEREPORT.PDF.

Key Community-Level Financial, Organizational, and Policy Challenges

Community data sharing is being recognized as a powerful way to positively affect the quality, safety, and efficiency of the care consumers receive. Gaining these benefits requires broad provider adoption, effective implementation, and associated changes in processes and structures. The potential to transform care delivery locally can be done without substantial regulations or community upheaval. The changes that accompany the expanded use of technology in health care pose challenges to longstanding assumptions and practices. SAHIEs should take a coordinated approach to addressing the challenges in an effort to achieve the broad benefits of data sharing. A well-planned and coordinated effort, sustained over time, can deliver improved results for providers and better serve consumers.

SAHIE planners need to share a common vision and purpose for sharing data.[25] Otherwise, conflicting ideas concerning the reasons participants should work together could stall the initiative. SAHIEs require a strong framework of participants that can make decisions that define and guide the data sharing effort. Resisting the temptation to address all challenges is likely to be difficult for most SAHIEs. Identifying and addressing key challenges, particularly in the early stages, is essential to managing available time and resources. Community data sharing initiatives must consider funding and sustainability once the initial investment has been depleted. They must also assign responsibility to a group of individuals around a common set of goals and for achieving a tangible result. All participants must agree on standards for policies, procedures, and system security controls.

[25] Sarath Malepati, et al., RHIOs and the Value Proposition, Value is in the Eye of the Beholder, *Journal of AHIMA 78*(3), March 2007. Available online at: http://www.nihcm.org/~nihcmor/pdf/RHIOsValueProp.pdf.

Stark Exception Opportunities

Issue

In August 2006, the U.S. Department of Health and Human Services promulgated final rules creating new information technology exceptions according to the Federal Stark law and safe harbors under the Federal Anti-Kickback statute.[26] The workgroup agreed that the regulations make it easier for hospitals to donate electronic prescribing technology and electronic health records to physicians, but noted little use by hospitals. The Stark exception and Anti-Kickback safe harbors for electronic prescribing are virtually identical. The regulations address the kinds of technology that can be donated, the technology standards, the kinds of organizations that may make donations, and the permitted methods of selecting recipients. The rule also addresses the permitted value of the technology, certain prohibited acts by both donors and physicians, the requirements for a written agreement, and a requirement that the donor not know or act in disregard of the fact that the physician already possessed equivalent technology.

Key Decisions

- Assess whether data sharing physicians qualify to receive technology under the Stark law exceptions from a permissible donor
- Validate that donated software is interoperable at the time it is provided to the physician and that it has been certified by the Certification Commission for Health Information Technology within twelve months prior to the date of donation
- Ensure that the donor has not taken any action to limit or restrict unnecessarily the use of technology, and that its use is not a condition of doing business with the donor
- Verify that the receiving physician pays at least 15 percent of the donor’s cost

Discussion

The revisions to the Federal Stark Law reflect an unprecedented degree of coordination between Centers for Medicaid and Medicare Services and the Office of Inspector General. This coordination reflects the government’s desire to remove impediments to the adoption of important, but expensive, software and related information technology that will enhance patient care and safety and reduce medical errors while simultaneously protecting federal health care programs from fraud, waste, and abuse. The workgroup viewed the changes in the regulations to allow hospitals to transfer the cost of select technology to physicians for much less than market value as a significant way to speed data sharing within communities.

[26] J. Phillip O’Brien, *HHS Announces New Federal Stark Law Exceptions and Federal Anti-Kickback Safe Harbors for Sharing Information Technology with Physicians,* Katten, Muchin, Rosenman, LLP, August 2006.
Available online at: http://www.kattenlaw.com/files/Publication/f7653806-4484-47c3-84bc-53e46dd2aa7f/Presentation/PublicationAttachment/01625f8c-d2ed-4783-b2fb-66ab4fa76305/hhs%20announces%20new%20federal%20stark%20law%20exceptions.pdf.

Establish Guidelines for Securing Local Community Funding

Issue

Community data sharing represents a public good and development efforts are mostly supported through in-kind contributions of participating providers. SAHIEs are actively engaged in transforming local health care processes burdened by paper, inefficiency, and redundancy. The workgroup agreed affordability is almost always cited as the primary barrier to data sharing. Providers often lack the financial capital to make an initial investment in technology. Implementing services on an incremental basis enables SAHIEs to minimize upfront investment costs. SAHIEs should explore grant opportunities, loans, and financing programs as a way to supplement startup costs. Allocating a portion of these funds to provide training and education to users of the technology is advisable to avoid safety and quality concerns.

Key Decision

- Investigate the possibility of applying for philanthropic funding or federal grant opportunities
- Evaluate the possibility for data sharing providers to form a partnership to seek community loans
- Investigate the potential of obtaining contributions from vendor partners to implement shared technology among community providers
- Evaluate funding opportunities from employers or civic groups within the community
- Consult with payers for consideration of funding for a demonstration project

Discussion

Obtaining financial support is a challenge that community data sharing initiatives must address, oftentimes to ensure sustainability. SAHIEs should devise a financial model that creatively explores funding through various sources to fully evaluate investment costs and revenue required to support the initiative. The financial model needs to include assumptions related to participant cost and value to the community addressing the benefits that pertain to each stakeholder.[27] Absent funding from an outside source, the workgroup suggested that communities approach data sharing conservatively and implement features on an incremental basis. In an incremental data sharing model, communities should carefully consider the data that needs to be shared electronically to provide the greatest coordination of care across delivery settings that enhance primary care and consumer involvement.

[27] In addition to the eHI Value Model, there are other useful tools available on the eHI website. Available online at: www.ehealthinitiative.org.

Establish Privacy and Security Boundaries

Issue

The benefits of appropriate data sharing among consumers and authorized providers are nearly universally understood and desired. Communities sharing data must develop a strategy to protect the privacy and security of electronic health information in a manner that builds upon the HIPAA Administrative Simplification provisions.[28] The workgroup felt that HIPAA provides an adequate framework for protecting health information and agreed that SAHIEs should implement additional data sharing protections. Resolving challenges related to privacy and security is essential in order to gain provider and consumer trust. Even a seemingly small misstep in this area can have serious implications for public trust and the credibility of the SAHIE.

Key Decisions

- Establish transparent provider and consumer data sharing control policies
- Disclose to stakeholders the frequency of user audits, the amount of data audited, and aggregate findings
- Identify data sharing integrity protocols and monitor users for compliance
- Identify security risk assessment parameters and appropriate monitoring controls
- Create a process to identify HIPAA privacy and security policies that require more stringent requirements
- Develop a process to inform consumers of their health information privacy and confidentiality rights in an open and transparent manner

Discussion

The issue of privacy and security is a major concern for all stakeholders. The success of community data sharing initiatives depends largely on consumer and provider willingness to trust that appropriate safeguards exist to protect the data. Given the pervasive concerns expressed by the consumer about unauthorized access and disclosure of their health information, it is critical that SAHIEs build consumer confidence in the protection of the data. The workgroup agreed that exchanging electronic health information, at the community level, holds great promise for a statewide health information exchange. The many possible benefits of data sharing will not be realized unless data sharing communities establish appropriate policy measures upfront.

[28] California HealthCare Foundation, *Privacy, Security, and the Regional Health Information Organization*, June 2007. Available online at: http://www.chcf.org/documents/chronicdisease/RHIOPrivacySecurity.pdf.

Identify and Organize a Community Advisory Group

Issue

Community data sharing initiatives require assembling an advisory group comprised of local stakeholders. The entities that would exchange the data typically form the leadership component of a SAHIE's advisory group. Essentially, any group of interested and motivated individuals can initiate the process. The workgroup felt that the advisory group should conduct a feasibility assessment to identify the potential benefits for the community. While it is not necessary to quantify these benefits at this stage, it is important for the advisory group to identify that there are benefits that accrue for the community as a whole that would justify continuing the initiative. Responsibilities of the advisory group involve addressing the complexities involved in exchanging data.[29]

Key Decisions

- Identify key community stakeholders to participate on a data sharing advisory group
- Nominate a subgroup of representatives tasked with directing the leadership of the advisory group
- Identify a strategy for developing a data sharing plan that takes into consideration the various community stakeholder needs
- Explore technology challenges that data sharing participants are likely to encounter for sharing data
- Facilitate the adoption of an efficient, well integrated, and universally accepted infrastructure that supports electronic health records
- Identify appropriate activities aimed at gaining an understanding of privacy and security issues unique to the data sharing community

Discussion

The long term sustainability of a community data sharing initiative requires a well articulated advisory group capable of engaging stakeholders and advancing the initiative into a functional process. The advisory group is one that provides structure and is able to carry the initiative forward through a potentially competitive environment created by virtue of the participating stakeholders. The participants must come to agreement on critical and potentially divisive issues such as protocols for patient identification and data transfer, data standards, rules for authentication, and access and data maintenance. The workgroup views building trust and collaboration among stakeholders as a leading challenge around data sharing.

[29] eHealth Initiative, *Health Information Exchange: From Start Up To Sustainability*, May 22, 2007. Available online at: http://ehr.medigent.com/assets/collaborate/2007/07/10/Health_Information_Exchange-Start_Up_to_Sustainability_Full_Report_07.09.2007001.pdf.

Ensure Implementation Activities Consider Provider Business Practices

Issue

Concerns about incidental or inappropriate release of data causes many providers to take a conservative approach to changing business policy and practices related to supporting data sharing. Data sharing initiatives can actually decrease provider efficiency if the participants choose to maintain dual workflows, one used for paper transactions and one for electronic transactions. Providers that exchange data must strive to identify and implement operational changes to streamline workflows for all communication types. The workgroup felt that providers need to analyze existing workflows and identify process changes that could be made to take advantage of the value achieved through data sharing. SAHIEs need to be sensitive to the restructuring of business practices for most participants as a result of increased use of technology.

Key Decisions

- Identify accreditation and certification standards for all hardware and software deployed by the data sharing community
- Develop a process to assess the range of existing business practices and workflows among participating provider organizations
- Develop a core set of data sharing workflow processes that can enhance the processes of data sharing participants
- Address data ownership issues that are likely to arise among data sharing participants

Discussion

Implementing a sustainable community data sharing model requires serious consideration and effort to establish policies around business practices related to exchanging electronic information. Developing a system that reduces the administrative burdens of the current paper-based system and replacing it with a more efficient process must be achieved.[30] The workgroup encourage SAHIEs to carefully evaluate business practices of the providers that are planning to engage in data sharing. SAHIEs should establish a data sharing model that provides the greatest business solution for the majority of participants. Harmonizing core data sharing business practices among participating providers will lay the foundation for building better electronic data sharing solutions.

[30] ProviderLink, *Creating RHIO's That Work: The Most Overlooked Five Pillars*, July 2005. Available online at: http://www.providerlink.com/documents/Creating%20RHIO's%20White%20Paper.pdf.

Alternate Community Data Uses

Secondary use of data can enhance health care for individuals, expand knowledge about disease and appropriate treatments, and support public health and security goals. In most instances, complex ethical, political, technical, and social issues impact the secondary use of data. A clear societal benefit exists to make local, state, and national health information available to communities for the purposes of early identification of communicable diseases and acute or long term population health threats.[31] Bioterrorism and outbreak response are not the only alternate uses of clinical data that can provide value to a community. Other secondary uses may allow researchers to better understand how various chronic illnesses affect different demographics of a particular community. SAHIEs need to develop sound policy coupled with stakeholder education to build community trust around the secondary uses of data.

Data sharing communities will need to establish a framework for the secondary use of data that includes a robust infrastructure of policies, standards, and best practices. Establishing such a framework can help guide and facilitate appropriate uses of secondary data and provide suitable protections for legitimate secondary use. The workgroup agreed that secondary use of data poses technical and policy challenges, and is pivotal to strengthening the health care system. Effective secondary use of data requires communities to develop a sufficient understanding of the inherent benefits and risks of using the data. SAHIEs must address the pressing issues related to the secondary use of data to build consumer trust in data sharing.

[31] Christina Davies, Rory Collins, Confidentiality and consent in medical records: Balancing potential risks and benefits of using confidential information, *British Medical Journal*, 333:349-351, August 12, 2006. Available online at: http://www.bmj.com/cgi/pdf_extract/333/7563/349.

Establish Transparency of Data Use beyond Treatment, Payment, and Healthcare Operations

Issue

An increasing demand for access to and analysis of data outside of the clinical setting exists today. In aggregate, secondary data is valuable for use in a broad range of applications for research, quality, public health, and consumer sectors. Anecdotal evidence suggests that the examination of aggregated data may facilitate early detection of emerging epidemics by the public health community. Educating consumers on the benefits and challenges of secondary data helps raise awareness and understanding of the ways that their information is being used.[32] The workgroup agreed that SAHIEs need to establish coherent policies and best practices for secondary use of data. Engaging consumers in dialogue, raising awareness, building collaboration, and clarifying issues are important steps for communities to implement for secondary uses of data.

Key Decisions

- Ensure the use of secondary data is conducted and managed through the use of an open and transparent process
- Educate consumers about the appropriate secondary uses of data
- Develop standard language on the secondary uses of data for data sharing participants to include in handouts and on relevant websites
- Conclude on a consumer consent process for the use of secondary data whereby a consumer can opt-in or opt-out of alternative data sharing
- Ensure that audit, compliance, notification of breaches, and escalation practices are in place
- Create a process regarding retention and destruction of data when used or created for secondary use

Discussion

Secondary data use must be conducted and managed solely through the application of open and transparent processes. Stakeholders should be engaged in a discussion to assure that these uses are undertaken with full disclosure. The responsibility for ensuring privacy and safeguarding data applies to the continuum of data users. Advances in technology and the ability to transmit data have resulted in data being used for multiple purposes other than direct care. SAHIEs will need to address questions concerning access and control of data. For the most part, consumers lack a clear understanding of data use beyond care delivery, and secondary data usage could easily be misunderstood. The workgroup agreed that explaining the benefits of secondary data use and the privacy and technical safeguards to the patient is a challenging task.

[32] American Medical Informatics Association, *Toward a National Framework for the Secondary Use of Health Data*, September 2006. Available online at: www.amia.org/inside/initiatives/healthdata.asp.

Identifying Privacy and Security Policies Governing Secondary Data Use

Issue

The increasing secondary use of data raises the need to define stakeholder rights and responsibilities. Establishing policies for the secondary use of data represents a huge challenge for community data sharing initiatives. The workgroup felt that SAHIEs should develop uniform data access, use, and control requirements for secondary data. At present, the level of data protection is significantly dependent on the stewardship of the provider. Data sharing introduces new issues and complexities that are non-existent in the paper environment. The value of secondary data is substantial, and appropriately de-identified data allows it to be accessed and used to a much larger extent because there is less need to control privacy protections.[33] Data that has been de-identified with no capability for re-identification can be readily disclosed, sold, or published without the risk of breaching personal rights to privacy.

Key Decisions

- Identify the approved uses of secondary data, and determine the community or other purposes that the data use may serve
- Define the technical safeguards that requestors of secondary data must have in place when submitting a request to obtain data
- Identify data elements to include in a de-identified secondary data set for appropriate limited uses
- Implement contracts and business associate agreements that specify the limited uses of secondary data
- Establish an appropriate data request policy for secondary data
- Adopt sound data stewardship practices addressing accountability, management, collection, viewing, sharing and disclosure, and enforcement of secondary data

Discussion

Understanding how a provider intends to use the data for alternate purposes and how that use will impact the community is critical. Issues related to secondary data access, use, and control require SAHIEs to approach the application of ongoing stewardship by first recognizing that health care is becoming consumer centric and that providers must put patients at the center of the decisions that are made about their information. This focus requires SAHIE commitment to continuously review policies, procedures, and practices in order that they clearly reflect the provider’s commitment to protecting data. The workgroup felt that SAHIEs must also reflect this philosophy in their consumer education, employee training, and policy and procedure enforcement.

[33] Ibid.

In Review

Service Area Health Information Exchanges (SAHIEs) are an important part in the emergence of broader health information exchange in Maryland. SAHIEs are typically made up of providers in a select geographic area that share the same patients across practices and settings. Exchanging clinical data within service areas establishes a foundation for connecting providers statewide. Enabling treating providers to share information about a consumer improves the overall safety, effectiveness, and efficiency of health care delivery. The Maryland Health Care Commission is working with providers to increase the efficiency and quality of care by facilitating communities to collaborate in ways to share clinical information electronically.

Planning data sharing requires conveners to conduct outreach and education that fosters growth and builds stakeholder trust. Community providers collaborating to exchange clinical information must work with stakeholders to resolve a number of issues in designing a data sharing model. For the most part, these issues relate to consumer control of the data, identifying technology that meets a minimum set of standards, and addressing various business practices that center on access, authentication, authorization, and audit. Collaboration among providers on technology and privacy and security policies play a significant role in communities that are planning to share clinical information.

Resolving the challenges of data sharing in a consistent manner is required in order to harmonize community implementation and increase the number of communities that exchange data. By adhering to the recommendations and guidance contained within this resource guide, SAHIEs can be assured that they have followed a rigorous process, incorporating both current and future requirements that address common technical standards and privacy and security protocols. Developing sound policy pertaining to privacy and security that is agreed upon within communities is an essential first step toward data sharing.

Many communities have expressed an interest in data sharing; some are currently in the planning stages while others have begun to share a limited amount of information electronically. The various challenges facing SAHIEs are not insurmountable and can, in fact, be addressed in a thoughtful and deliberate manner to satisfy all stakeholders. The promise of data sharing is undoubtedly worth the efforts involved. As this resource guide has attempted to illustrate, every data sharing challenge has a solution, and those solutions can be supported through technology, sound policy development, and best practices.

APPENDIX A

Workgroup Participants and Key Contributors

Douglas Abel
Chief Information Officer
Anne Arundel Medical Center

Raymond Adkins
Chief Information Officer
Peninsula Regional Medical Center

Salliann Alborn
Chief Executive Officer
Community Health Integrated Partnership

Jama Allers
Practice Consultant
MedChi, The Maryland Medical Society

Karen Barker
Vice President, Chief Information Officer
LifeBridge Health

Richard Boehler, MD
Chief Medical Officer
St. Joseph Medical Center

Kevin Burbules
Chief Information Officer
Civista Medical Center

Rick Casteel
Vice President of Information Technology
Upper Chesapeake Health

Mark DeVault
Director of Information Technology
Dorchester General Hospital

Kathleen Dyer
Vice President, Chief Information Officer
Adventist Healthcare

Rick Edwards
Senior Director, Chief Information Officer
Howard County General Hospital

John Eichensehr
Director, Information Technology
Quest Diagnostics Incorporated

Michelle Green Clark
Project Director, State Office of Rural Health
Department of Health and Mental Hygiene

Karen Gerner
Privacy and Security Officer
Holy Cross Hospital

William Greskovich
Vice President of Operations, Chief Information Officer
St. Agnes Hospital

Ed Grogan
Vice President, Chief Information Officer
Calvert Memorial Hospital

David Horrocks
Senior Vice President
Erickson Retirement Communities

Alan Johnson
Chief Information Officer
Doctors Community Hospital

Stephen Johnson
General Counsel, Director of Law & Advocacy Division
MedChi, The Maryland Medical Society

Leta Kajut
Director, Health Information Exchange Technology
Primary Care Coalition of Montgomery County

Mary Jane Kamps
Vice President, Chief Information Officer
Union Hospital

Dennis Lilik
Chief Information Officer
Dimensions Health System

Carey Leverett
Vice President, Information Systems
Washington County Health System

Kim Moreau
Assistant Vice President of Information Systems
Carroll County Hospital Center

DeWayne Oberlander
Executive Director
Columbia Medical Practice

Manuel Ocasio
Vice President, Chief Information Officer
Holy Cross Hospital

Murray Oltman
Director of Information Services
Atlantic General Hospital

Traci Phillips
Director, Health Care Finance
Maryland Hospital Association

Stephen Prouse
Director of Clinical Applications
Upper Chesapeake Health

Sanjay Purushotham
Executive Director of Information Services
Bon Secours Hospital

David Quirke
Vice President, Chief Information Officer
Frederick Memorial Hospital

Denise Reeser
Managing Principle
Health Care Information Consultants

Carol Richardson
Privacy Officer
The Johns Hopkins HIPAA Office

Bart Rowe
Senior Director, Information Technology
Baltimore Washington Medical Center

Catherine Szenczy
Senior Vice President, Chief Information Officer
MedStar Health

Donald Sirk
Director of Information Technology
St. Mary’s Hospital

Tressa Springmann
Vice President, Chief Information Officer
Greater Baltimore Medical Center

Allison Trumpy
Director, Information Technology
Chester River Hospital Center

Daniel Wilt
Vice President of Information Technology
Erickson Retirement Communities

MARYLAND
HEALTH CARE
COMMISSION

Marilyn Moon, Ph.D., Chair

Rex W. Cowdry, M.D., Executive Director

David Sharp, Ph.D., Director
Center for Health Information Technology

4160 Patterson Avenue
Baltimore, MD 21215
Tel: (410) 764-3460
Fax: (410) 358-1236
www.mhcc.maryland.gov