Privacy & Security

Solutions & Implementation Activities

For a Statewide
Health Information Exchange

September 2008

Marilyn Moon, Ph.D.
Chair

Rex W. Cowdry, M.D.
Executive Director

MHCC | MARYLAND HEALTH CARE COMMISSION

4160 Patterson Avenue
Baltimore, Maryland 21215

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.

(BLANK PAGE)

Privacy & Security

Solutions & Implementation Activities

For a Statewide Health Information Exchange

(BLANK PAGE)

Table of Contents

Executive Summary 1
Background 2
Privacy and Security Project Overview 2
Report Limitations 2
Sector Group Privacy and Security Practices 2
Guiding Principles 4
Identification of Key Barriers 5
State and Federal Privacy and Security Initiatives 8
Privacy and Security Initiatives at the Federal Level 8
Health Information Technology Development in Maryland 9
HIT Initiatives in Bordering States 11
Involvement in National Health Information Technology Initiatives 12
Principles, Barriers, and Solutions 14
Accessibility 14
Consumer-Centric Exchange 16
Emergency Access 18
Governance 20
Misuse 22
Security 24
Standards 26
Sustainability 28
Implementation Activities 31
Accessibility 31
Consumer-Centric Exchange 31
Emergency Access 32
Governance 33
Misuse 33
Security 34
Standards 34
Sustainability 34
Desired Future State 36
Accessibility 36
Consumer-Centric Exchange 36
Emergency Access 36
Governance 37
Misuse 37
Security 37
Standards 37
Sustainability 38
Looking Ahead 39
Acknowledgements 39
Appendix A 40
Solutions and Implementation Participant List 40

(BLANK PAGE)

Executive Summary

The Maryland Health Care Commission (MHCC) convened a Solutions and Implementation Workgroup (Workgroup) to formulate solutions and develop implementation activities that address organization-level business practices affecting statewide privacy and security policies in order to support interoperable health information exchange (HIE). The Workgroup consisted of individuals representing multiple stakeholder groups, including consumers, hospitals, long term care facilities, medical laboratory and diagnostic imaging centers, payers, pharmacies, physicians, and purchasers. Workgroup participants developed guiding principles for exchanging patient information electronically, and evaluated privacy and security barriers to HIE that impact all stakeholder groups. The Workgroup also evaluated the impact of these barriers on the guiding principles, and proposed implementation activities to guide the development of HIE in Maryland.

Barriers identified by the Workgroup included: access to data, a common patient identifier, concerns regarding the use of data, funding, interoperability, liability, stakeholder trust, and technical and process infrastructure. Workgroup participants agreed on a set of guiding principles perceived as critical to the electronic exchange of patient information. Key guiding principles included: accessibility, consumer-centric exchange, emergency access, governance, misuse, security, standards, and sustainability. These principles and barriers provided the framework for the solutions developed by the Workgroup.

The Workgroup agreed on a number of proposed solutions that included making electronic health information accessible to all stakeholders when appropriate, ensuring that consumers control the flow of their information, establishing rules for emergency access to patient information, embracing a governance that is inclusive and transparent, defining penalties for the misuse of electronic health information, assuring that data security protects patient privacy, developing exchange standards, and establishing a well-defined value proposition and equitable business model. The implementation of these solutions will guide efforts to establish a statewide HIE. The Workgroup assembled a list of implementation activities that they believed would steer HIE to a desired future state.

Resolving concerns about privacy and security is essential to building consumer trust in the electronic storage and exchange of health information. HIE offers many advantages over the current system of sharing patient information. Comprehensive medical information about the patient can be available at the time and place of care, and can be linked to clinical decision support systems and information regarding quality, outcomes, and cost. Accurate and available information empowers both patients and providers, and promotes evidence-based care that is based on demonstrated value.

HIE offers the possibility of making clinical and health services research more relevant and less costly, and can provide for cost-effective analysis of adverse drug effects, biological threats to homeland security, and emerging infectious diseases. By ensuring stakeholder involvement in the development and execution of a strategy to advance health information technology, MHCC expects to increase the use of electronic health records and facilitate the development of a private and secure consumer-centric HIE in Maryland.

Background

Privacy and Security Project Overview

In 2007, the Maryland Health Care Commission (MHCC) convened a group of stakeholders to identify barriers to health information exchange (HIE) and recommend solutions to those barriers. This initiative emerged out of the privacy and security work of eight Sector Groups from the prior year. These Sector Groups were asked to assess business policies and practices in general, and privacy and security policies and practices in particular, that may impede the implementation of HIE in Maryland. Findings from the Sector Groups are available on the MHCC website.[1] A Solutions and Implementation Workgroup (Workgroup) was subsequently formed with representatives from each Sector Group. Participants were asked to formulate solutions and implementation activities building on the work of the Sector Groups.[2]

The Workgroup agreed upon a set of principles that would help guide the development of solutions and implementation activities, and identified barriers that impacts all the Sector Groups. As part of the work effort, the Workgroup aligned the barriers to the guiding principles, deliberated on their impact to HIE, and formulated solutions and implementation activities. Information contained in this report can be used to develop detailed implementation plans to address the key barriers that impede the implementation of HIE in Maryland.

Report Limitations

This report builds on the findings from the privacy and security initiative of the Sector Groups from the prior year. Information included in this report represents the views of Workgroup participants. This report addresses a defined set of privacy and security barriers related to HIE in Maryland. Developing detailed implementation work plans will be the challenge for others that share in the commitment to implement a private and secure data exchange. The implementation activities presented in this report will guide the development of a consumer-centric HIE.

Sector Group Privacy and Security Practices

MHCC conducted an assessment of privacy and security policies and business practices related to HIE from the perspective of eight Sector Groups. These Sector Groups represented consumers, hospitals, long term care, medical laboratories and diagnostic imaging centers, payers, pharmacies, physicians, and purchasers. Key stakeholder findings from each of the Sector Groups are summarized below.

Consumer Sector

Stakeholders are concerned that current protections to maintain the confidentiality of patient information are not sufficient to protect paper records; these concerns increase dramatically

[1] Available at: http://mhcc.maryland.gov/electronichealth/assess_privacy_security.pdf.
[2] A complete list of Workgroup participants can be found in Appendix A of this report.

when applied to electronic patient information. Stakeholders noted inconsistencies in provider interpretation of the HIPAA privacy regulations. Stakeholders also felt that they should control the use and disclosure of their electronic health information. General agreement existed around the need for greater protection of electronic patient information.

Hospital Sector

Stakeholders agreed that while a business case for HIE exists, most hospitals are currently focused on connecting internal disparate systems. In general, hospitals are exploring opportunities for exchanging patient data with service area providers, but are concerned about exchanging patient data with other hospitals. Hospitals perceive data as critical to maintaining their market share. Stakeholders agreed that electronic patient information can increase the quality and efficiency of care delivery. Hospitals cited the lack of consistent business practices and privacy and security policies, as well as financial costs, as barriers to implementing HIE.

Long Term Care Sector

Stakeholders noted variations in the use of technology as the most significant barrier to HIE. High employee and patient turnover, as well as low reimbursement, were considered the main reasons for slow technology growth in this sector. Stakeholders believe that HIE will allow improvements in patient care, rapid access to test results, and increased efficiency in care delivery. Greater education and awareness regarding the benefits of HIE to long term care were viewed as essential for advancing the use of technology throughout the industry. Stakeholders also viewed the lack of privacy and security policies as a key barrier to implementing HIE.

Medical Laboratory and Diagnostic Imaging Center Sector

Stakeholders expressed a general concern about the lack of technology that exists in most physician practices. An infrastructure that supports HIE could reduce the number of costly provider connections currently needed to support different provider technologies. Storing and forwarding images creates administrative challenges for most stakeholders. Concerns were raised over the lack of national and local privacy and security policies, potential consumer resistance, and the level of disparities in technology adoption across sectors. Stakeholders also expressed concerns about revenue declines if duplicate testing is eliminated as a result of HIE.

Payer Sector

Stakeholders expressed uncertainty about the value proposition of HIE, and questioned whether the benefits of HIE accrue primarily to payers as compared to the other Sector Groups. The cost of implementing systems to support HIEs, and the length of time required to realize a return on investment, were concerns of this group. Stakeholders could not agree whether implementing an HIE at the present time was a sound decision. They did agree that more planning would be an appropriate next step for HIE in Maryland. Stakeholders also expressed concern over the lack of statewide privacy and security policies.

Pharmacy Sector

Stakeholders reported that HIE can eliminate the use of paper prescriptions, improve patient safety, and increase the efficiency of filling prescriptions. Consensus existed among stakeholders that sound privacy and security policies are needed before they would feel secure in participating in an HIE. They also raised concerns regarding physician reluctance to use technology, as evidenced by the slow adoption of electronic prescribing. Stakeholders felt that physician reluctance to implement technology would negatively impact HIE implementation in Maryland.

Physician Sector

Stakeholders agreed that HIE would reduce medical errors, increase operating efficiencies, advance pay for performance initiatives, and allow for more consistent use of evidence-based medicine. Almost all stakeholders raised concerns about reduced productivity during technology deployment and the increased liability exposure with HIE. Stakeholders were in agreement that incentives to adopt health information technology (HIT) are misaligned, and encouraged the State to consider financial incentives to expand technology adoption. The lack of privacy and security policies were troubling to most stakeholders.

Purchaser Sector

Stakeholders noted that while they were likely to benefit from improvements in the health status of their employees, this benefit will not be realized until well after an HIE is implemented. Some concerns were expressed about the ability of purchasers to participate in HIE funding. Stakeholders considered the lack of privacy and security policies as the leading barriers to implementing HIE, followed closely by the costs associated with purchasing or upgrading existing computer systems, and hiring additional staff.

Guiding Principles

The Workgroup identified eight guiding principles to HIE: accessibility, consumer-centric, emergency access, governance, misuse, security, standards, and sustainability. A brief description of the eight guiding principles is discussed below.

- ***Accessibility*** – Access to patient data where and when it is needed is essential to the success of a HIE. Improving health care quality, as well as enhancing coordination of patient care, can only be realized when patient information is appropriately shared at the health care delivery site.

- ***Consumer-Centric*** – A consumer-centric HIE ensures that consumer interests guide decision-making. Generally speaking, HIE expands the amount of patient information available to a greater number of health care stakeholders. In a consumer-centric HIE, under most circumstances, the flow of data is controlled by the consumer.

- ***Emergency Access*** – An HIE must appropriately manage access to patient information in emergent situations. Emergency circumstances must be clearly defined, and patients need to be notified when providers are granted emergency access to data. A core data set for use in emergency situations needs to be defined.

- ***Governance*** – A governance body defines the policies and technical infrastructure of an HIE. Decisions made by the governance body are guided by the need to keep patient information private and secure. Broad stakeholder participation builds trust and ensures that all stakeholder views are included in the decision-making process.

- ***Misuse*** **–** Policies and procedures are needed to limit the potential for patient information to be used and disclosed inappropriately. It is critical that protocols for the routine use of patient data are established, and formal penalties for misuse are developed. Well-defined policies for controlling how patient information is used and disclosed builds stakeholder trust in the HIE.

- ***Security*** **–** Physical and technical safeguards to protect patient data whenever and wherever it is accessed, used, or disclosed are fundamental to sharing information. Ensuring the security of patient information is essential to the success of HIE. Policies relating to access, authorization, authentication, and audit are required for exchanging patient data electronically.

- ***Standards*** **–** HIE requires stakeholders to agree on an acceptable range of standards and a mechanism to control for versioning within the standards. Defining standards that facilitate interstate and intrastate data sharing is critical. Implementing too many standards can add unnecessary complexity, while adopting too rigid standards can hinder HIE participation.

- ***Sustainability*** **–** A business model that provides value to stakeholders, particularly a value that they are willing to pay for, is critical to the success of an HIE. Identifying a value proposition for each stakeholder encourages wide-spread participation. Creating a value proposition that will generate sufficient stakeholder interest to participate in an HIE is a significant challenge.

Identification of Key Barriers

The Workgroup focused their initial efforts on reviewing the barriers to implementation of an HIE, as identified by the Sector Groups. The Workgroup reached agreement on eight barriers: access to data; a common patient identifier; concerns regarding the use of data; funding; interoperability; liability; stakeholder trust; and technical and process infrastructure. A general description of each barrier is discussed below.

Access to data

Defining appropriate access to patient information requires an assessment of the circumstances under which data can be accessed.[3] Determining the parameters surrounding access to electronic health information for routine disclosures, public health, marketing, biosurveillance, etc., requires stakeholders to agree upon appropriate use and disclosure policies. Tracking access to patient data will ensure adherence to these policies. Monitoring access to data is particularly critical when the information pertains to sensitive diagnoses, such as HIV, substance abuse, genetic testing data, or mental health disorders.[4]

[3] Illinois Health Information Security and Privacy Collaboration Legal Workgroup meeting minutes, September 26, 2007, available at: http://www.idph.state.il.us/hispc2/lwg/LWG%20Mins%209%2026%2007.pdf.
[4] Ibid.

Common Patient Identifier

Patient identifiers are widely used by providers to access patient information for administrative and clinical purposes.[5] These identifiers are unique to each organization and are used for both paper and electronic patient records. Although exact patient matching continues to be a challenge, algorithms can be established to match patient information across disparate HIT systems. Attempts to establish a single patient identifier have consistently met with public outcry due to privacy and security concerns. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) initially included a provision to establish a standard unique health identifier for individuals. Several years of controversy and protest by privacy advocates resulted in Congress withholding funding for a unique patient identifier.[6]

Concerns regarding the use of data

Expanding the use of patient information from paper to electronic formats increases stakeholder concerns about how data is used. Privacy advocates have pointed to numerous examples of inappropriate use of patient information for purposes such as commercial marketing campaigns, denial of employment or insurance coverage, and identity theft. Secondary uses of electronic health information for public health also raise concerns in the minds of many consumer privacy advocates.[7] While secondary uses are primarily for the public good, the benefits and risks of secondary use of data, questions regarding data ownership, and public consent issues need to be addressed.

Funding

The number of HIE initiatives is increasing nationally; however, efforts to implement a sustainable business model have not been successful. A March 2007 survey of 38 HIEs identified funding from federal, state, and private foundation grants as the primary source of startup funding, and indicated that most HIEs tend to depend on funding from membership fees rather than transaction-based fees.[8] The report also found that HIEs in general have not pursued ongoing funding opportunities from local or regional private foundations.[9]

Interoperability

The inability of HIT systems to be interoperable can be attributed in part to a lack of incentives, privacy and security policies, and inconsistent use of standards. Resolving issues related to vendor incompatibilities due to product versioning is a notable challenge for nearly all stakeholders. Adding to the challenge of interoperability are the multiple communication

[5] Appavu, Soloman I., *Analysis of Unique Patient Identifier Options, Final Report*, Department of Health and Human Services, November 24, 1997.

[6] The National Alliance for Health Information Technology (NAHIT), *A Timeline of the Unique Patient Identifier*, available at: http://www.nahit.org/dl/docs/Timeline_of_the_Unique_Patient_Identifier.pdf.

[7] Safran, Charles, et al., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, Journal of the American Medical Informatics Association, 14:1-9, 2007. DOI 10.1197/jamia.M2273, available at: http://www.jamia.org/cgi/reprint/14/1/1.pdf.

[8] Christopher, Michael and Jensen, Martin, *Sustainable RHIO Funding and the Emerging Business Model, Annual Survey of Regional Health Information Organization Finance*, *Findings*, *Public Summary of Report*, September 2007, available at: http://www.hittransition.com/rhio2007/PublicSummary_2007SurveyReport.pdf.

[9] Ibid.

protocols, data formats, vocabularies, languages, and character sets used.[10] Exchanging patient data electronically and merging the data into electronic health records (EHRs) without manual intervention requires addressing the challenges surrounding policy and technology.

Liability

Sharing patient information electronically raises questions regarding the duty of providers to appropriately use the information when rendering care. Providers often express concerns about their obligation to review significant amounts of electronic patient data, as well as the implications of possibly reviewing only recent episodic information. Data manipulation fears are also a factor when reviewing data from another source. Providers will likely avoid exchanging electronic patient information until they are assured that increased information expands their knowledge but not their liability.

Stakeholder Trust

A perceived loss of control, as well as stakeholder concerns regarding threats to competitive interests, can easily invoke distrust. Building stakeholder trust takes time and is generally accomplished by defining common goals, maintaining open communication, securing stakeholder engagement, securing a public-private governance, creating a roadmap, and initiating a shared business model.[11] Data sharing requires transparency about what information is being shared and why the information is being shared. Transparency is critical to securing stakeholder confidence that data is exchanged for legitimate reasons.

Technical and Process Infrastructure

An inclusive and transparent governance body with broad stakeholder representation is essential to implementing an infrastructure that can effectively address the policy and technology challenges of an HIE. Among other things, the governance body is tasked with developing a business plan and establishing a sustainable infrastructure. A sound infrastructure can ensure that the HIE appropriately responds to challenges related to finance, policy, and technology. On the other hand, a poorly conceived business plan that fails to anticipate the complexity of the infrastructure negatively impacts on the sustainability of an HIE.

[10] Moen, William E., *Barriers to Interoperability – Technical and Not So Technical*, (5th Annual GILS Conference, April 7-10, 2003), Lisle, IL.

[11] Burchell, Leigh, *Ten Tips for Facilitating Community Health Information Exchange*, Advance for Health Information Executives, Merion Publications, 2008, available at: http://health-care-it.advanceweb.com/editorial/content/editorial.aspx?cc=93847.

State and Federal Privacy and Security Initiatives

Privacy and Security Initiatives at the Federal Level

Health information resides in multiple provider settings and exists in both paper and electronic formats. The various policies, technology, and business practices that are common across care settings creates challenges for exchanging electronic health information. The Federal government has developed multiple programs aimed at addressing these variations, which have served as a framework for several of the HIT initiatives in Maryland. Key Federal projects are summarized below.

Office of the National Coordinator for Health Information Technology

To improve health care quality and efficiency, a Presidential Executive Order was issued in 2004 that provided a framework to develop and implement a nationwide interoperable HIT infrastructure.[12] A key component of this executive order was the establishment of the Office of the National Coordinator for Health Information Technology (ONC), within the Department of Health and Human Services (HHS), to lead and coordinate efforts for the development and nationwide implementation of an interoperable HIT infrastructure to improve the quality, safety, and efficiency of health care. An underlying principle of the ONC is that electronic patient information needs to be secure and protected.

American Health Information Community

In 2005, the Secretary of HHS established the American Health Information Community (AHIC) as a federal advisory body to coordinate activities and speed HIT adoption. AHIC consists of 18 members, including the Secretary of HHS and 17 members from the public and private sectors. The AHIC established seven workgroups to analyze HIT issues and make recommendations to the Secretary. The AHIC is planning a transition to a successor entity, also known as AHIC 2.0, at the end of 2008. This consortium is expected to operate as a public-private partnership, function independently, and be self-sustaining as it continues its work to support the implementation of an interoperable nationwide health information exchange.[13]

Health Information Security and Privacy Collaboration

In 2005, HHS awarded a contract to RTI International and the National Governor's Association (NGA) to establish the Health Information Security and Privacy Collaboration (HISPC), an initiative to assess the privacy and security barriers to the development of interoperable health information exchange across states. HISPC participants identified the following key barriers to HIE: variations in business practices and in the interpretation of HIPAA's administrative simplification regulations, inconsistent administrative and physical safeguards, the lack of standard authentication and authorization procedures, inadequate auditing capability of software

[12] The White House Office of the Press Secretary, *Executive Order: Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator,* Washington, D.C., April 27, 2004.

[13] Information available on the American Health Information Community website at: http://www.hhs.gov/healthit/community/background/.

applications, the inability to accurately match patient records, inadequate investment in security infrastructure, the lack of stakeholder trust, and conflicting federal and state laws pertaining to HIE.[14]

Healthcare Information Technology Standards Panel

In 2005, through the ONC, HHS awarded contracts to establish the Healthcare Information Technology Standards Panel (HITSP), a public-private sector partnership with a goal to develop a ". . . widely accepted and useful set of standards specifically to enable and support widespread interoperability among health care software applications, as they will interact in a local, regional and national health information network for the United States."[15] HITSP is developing a harmonization framework that defines interoperability specifications, transactions, transaction packages (logical groupings of transactions), and components (logical grouping of base standards, including messaging and terminology). The development of HITSP recommendations are guided by the priorities and use cases defined by the AHIC.[16]

Health Information Technology Development in Maryland

HIT adoption in Maryland parallels the level of adoption and implementation activities that are occurring nationwide. A joint project of the Robert Wood Johnson Foundation and the ONC estimated that about 24.9 percent of physicians and hospitals use EHRs,[17] which anecdotally, is about the same rate of adoption in Maryland. Recent HIT initiatives in Maryland include: the Centers for Medicare & Medicaid Services (CMS) Electronic Health Record (EHR) Demonstration Project, the Doctor's Office Quality Information Technology (DOQ-IT) EHR adoption project, Harmonization of Service Area Health Information Exchange policies, the HIT Demonstration Project, the Task Force to Study Electronic Health Records, and the planning for a statewide HIE. A brief summary of these initiatives is presented below.

CMS EHR Demonstration Project

CMS is implementing a five-year demonstration project (project) to encourage small to medium-sized primary care physician practices to adopt and utilize EHRs to improve the quality of patient care. The project is designed to demonstrate that adoption and use of EHRs will reduce medical errors and improve the quality of care. The project will provide financial incentives over a five-year period to about 1,200 physician practices across the country that use an EHRs certified by the Certification Commission for Health Information Technology to improve quality. The Maryland State Medical Society, MedChi, MHCC, and the District of Columbia Medical Society were selected as one of 12 community partners to participate in the project, which is scheduled to begin in September 2008.

[14] Ibid, pp. ES-4-ES-8.

[15] Information available on the Healthcare Information Technology Standards Panel (HITSP) website at: http://www.hitsp.org/default.aspx.

[16] Ibid.

[17] Jha, Ashish K., et al., *How Common Are Electronic Health Records In The United States? A Summary Of The Evidence,* Health Affairs, November/December 2006; 25(6): p. w496-w507.

DOQ-IT Summary

The DOQ-IT program was established to provide support to adult primary care physicians wishing to acquire, implement, and utilize EHRs in order to improve patient care, safety, and practice workflow.[18] Delmarva Foundation, a Maryland-based non-profit organization, was awarded a three-year contract by the CMS to recruit and develop educational material for small-to medium-sized adult primary care practices seeking to implement an EHR. The Delmarva Foundation recruited 43 primary care practices in Maryland to participate in DOQ-IT; the contract ended in July 2008.

Harmonization of Service Area Health Information Exchanges

MHCC has convened hospital chief information officers and other key stakeholders to identify and reach consensus on the range of policies and business practices for community-centric HIEs. The harmonization of service area health information exchange (SAHIE) efforts in the state will minimize the difficulties in connecting to a statewide HIE. Information derived from this effort will provide a framework for policies that can be used by planning teams to address statewide privacy and security policies for electronic health information. The project will also identify a set of compatible standards for exchanging data between hospitals and other health care providers.

HIT Demonstration Project

In support of Governor Martin O'Malley's goal to improve health care quality and safety through the creation of a statewide electronic HIE, CareFirst BlueCross BlueShield (CareFirst) has provided funding for two Maryland HIT initiatives. CareFirst has agreed to provide approximately $967,000 to the Community Health Integrated Partnership (CHIP), a Human Resources and Services Administration (HRSA) sponsored Health Center Controlled Network. CHIP is building a management services data center for EHRs. CareFirst also agreed to fund approximately $550,000 to LifeBridge Health, a Maryland health system that includes Sinai Hospital, Northwest Hospital Center, Levindale Hebrew Geriatric Center and Hospital, and the Jewish Convalescent and Nursing Home, to electronically link consumers and health care providers.[19] EHR adoption is a prerequisite to for HIE; CareFirst will consider funding additional HIT demonstration projects in the fall of 2008.

Task Force to Study Electronic Health Records

The Task Force to Study Electronic Health Records (Task Force) was established by the Maryland General Assembly during the 2005 legislative session. The Task Force consisted of 26 members appointed by the Governor representing a broad range of interests in health care and HIT. The Task Force was required to study electronic health records, and the current and potential expansion of electronic health record utilization in Maryland. The Task Force studied several issues that included electronic transfer, electronic prescribing, computerized provider order entry, and the cost of implementing these functions. The Task Force also examined the impact of the current and potential expansion on school health records, patient safety, and

[18] DOQ-IT information available on the Delmarva Foundation website at: http://www.delmarvafoundation.org/providers/physicians/DOQ-IT/index.html.

[19] CareFirst, *Press Release: Advancing the Use of Health Information Technology in Maryland*, February 12, 2008, available at: http://www.carefirst.com/media/NewsReleasesDetails/NewsReleasesDetails_20080212.html.

privacy. The Task Force submitted a final report to the Governor and the Legislature on December 31, 2007.[20] MHCC is actively implementing several of the Task Force recommendations.

Two-Phase Implementation of a Statewide HIE

MHCC and the Health Services Cost Review Commission (HSCRC) developed a two-phase strategic plan to implement a consumer-centric statewide HIE. The first phase, a planning phase, involves two multi-stakeholder groups assembled to resolve policy issues and address technical and operational challenges of building a statewide data exchange in Maryland. The Chesapeake Regional Information System for our Patients and the Montgomery County Health Information Exchange Collaborative are expected to submit a report in February 2009. The second phase, an HIE implementation phase, is expected to begin during the third quarter of 2009, and will incorporate the best ideas from the two groups.

HIT Initiatives in Bordering States

Maryland residents obtain health care from providers both within the state and from providers in surrounding states, which include Delaware, Pennsylvania, Virginia, and West Virginia. Keeping pace with bordering states ensures continuity in data sharing with those neighboring states. In a survey conducted by the NGA, the governors of Delaware, Pennsylvania, Virginia, and West Virginia, as well as the governors of other states participating in the survey, agreed that the development of HIEs, and the policies that promote interconnectivity for local and state-level HIEs, are top priorities over the next two years.[21] An overview of HIT initiatives among bordering states is described below.

Delaware

In October 2006, the state awarded a contract to build a statewide HIE in Delaware, which will provide physicians with real-time electronic access to patient data.[22] The Delaware Health Information Network (DHIN) is a public-private partnership that provides the organizational infrastructure to support the exchange of patient information across the state. In 1997, Governor Thomas Carper signed into law legislation to develop a community-based health information network. Physicians, hospitals, commercial laboratories, community organizations, and patients will be able to participate in the DHIN when it is fully implemented.

Pennsylvania

In 2005, industry, academic, and government leaders in Pennsylvania supported the establishment of the Pennsylvania Health Information Exchange to advance interoperable clinical data exchange throughout Pennsylvania. Efforts in 2007 were expanded to advance projects for e-prescribing, e-radiology, medical innovations, Health Level 7 interface projects, and interoperable health records. In March 2008, Governor Edward Rendell signed an Executive

[20] *The Final Report of the Task Force to Study Electronic Health Records*, available at: http://mhcc.maryland.gov/electronichealth/presentations/task_force_rpt123107.pdf.

[21] Smith, Vernon K. et al., *State e-Health Activities in 2007: Findings from a State Survey*, The Commonwealth Fund, February 2008, p. ix.

[22] Delaware Health Information Network (DHIN), information available on the DHIN website at: http://www.dhin.org/.

Order creating a governance structure to oversee building of the Pennsylvania Health Information Exchange.[23]

Virginia

In January 2008, Governor Timothy Kaine awarded funding to Centra Health System in Lynchburg and the Northern Virginia Regional Health Information Organization (NOVARHIO) for specific HIT projects. Centra Health plans to extend electronic records functionality to provide local physicians with access to quality measures and clinical best practices. NOVARHIO plans to provide electronic access to patient medication histories in hospital emergency rooms and educate local citizens about the value of personal health records. In 2006, Virginia also awarded HIT grants to CareSpark, based in Virginia and Tennessee, the Community Care Network of Virginia, a network of federally qualified health centers, and Richmond-based MedVirginia.[24]

West Virginia

In June 2006, Governor Joe Manchin established the West Virginia Health Information Network, a public-private partnership to advance the design, implementation, operation, and maintenance of an interoperable patient data network. The network will support and facilitate secure electronic access to laboratory and radiology results, medical record information transfer, disease management, surveillance, and reporting, physician order entry, prescription drug tracking, drug and allergy interaction alerts, and secure electronic consultations between providers and patients.[25] Another initiative in West Virginia is the HEALTHeWV, which is aimed at providing a web-based electronic medical records system to improve health care in rural communities using chronic disease and prevention management tools.[26] Lastly, the West Virginia eHealth Initiative (WVeHI) works with providers, health insurers, businesses, and government to advance adoption of information technology to improve the quality, efficiency, and safety of health care.[27]

Involvement in National Health Information Technology Initiatives

MHCC is actively participating in several national HIT initiatives to ensure that statewide data sharing efforts remain consistent with national activity. The national initiatives include the American Health Information Community, Certification Commission for Health Information Technology, the Multi-State Collaborative on Standards Policy Adoption, and the Privacy and Security Taskforce of the State Alliance for e-Health. An overview of these initiatives is provided below.

[23] Health Data Management, *Pennsylvania Seeks Statewide HIE*, March 27, 2008, available at: http://www.healthdatamanagement.com/news/HIE25964-1.html.

[24] Hayes, Heather B., *Virginia makes two grants for innovative uses of health IT*, Government Health IT, January 29, 2008, available at: http://www.govhealthit.com/online/news/350201-1.html.

[25] West Virginia Health Information Network (WVHIN), information available on the WVHIN website at: http://www.wvhin.org/home.aspx.

[26] HEALTHeWV, *HEALTHeWV Program*, information available on the HEALTHeWV website at: http://www.healthewv.net/program/.

[27]The West Virginia eHealth Initiative (WVeHI), *Overview: WV e-Health Initiative (WVeHI)*, information available on the WVeHI website at: http://www.wvehi.org/overview.asp.

American Health Information Community

MHCC participates on the American Health Information Community (AHIC) Privacy and Security Workgroup and on occasion with the Consumer Empowerment and EHR Workgroups. AHIC established seven Workgroups to provide input and make recommendations to facilitate implementation of digital and interoperable health records, while ensuring that the privacy and security of patient records are protected.[28] AHIC meetings are open to the public with public comments actively solicited after each meeting.

Certification Commission for Health Information Technology

MHCC participates on the Network Workgroup of the Certification Commission for Health Information Technology (CCHIT). CCHIT is a voluntary, private-sector organization formed in July 2004 with a mission to accelerate the adoption of HIT by creating an efficient, credible and sustainable network and product certification program. As of August 2008, CCHIT has certified the products of 92 ambulatory and 14 inpatient EHR vendors. The Network Workgroup is defining certification criteria for networks, establishing testing procedures, and developing a roadmap to expand certification criteria in the future. The network certification program is scheduled to begin in October 2008.

Multi-State Collaborative on Standards Policy Adoption

MHCC participates in the *Multi-State Collaborative on Standards Policy Adoption*, a HISPC project that will ". . . establish guiding principles for the minimal privacy and security parameters necessary for effective interstate and intrastate interoperability through elaboration of a health care privacy and security constitution . . . ."[29] The collaboration is expected to define HIPAA-compliant business practices and standards that HIEs can adopt to share information with authorized and authenticated providers in other states. The project will address the minimal audit standards and procedures to assure appropriate identification, including access control and authentication for interstate HIE.

Privacy and Security Taskforce of the State Alliance for e-Health

The NGA Center for Best Practices established the State Alliance for e-Health (State Alliance) to coordinate and explore HIT initiatives and the challenges of implementing an HIE. Maryland is participating in the State Alliance's Privacy and Security Taskforce, which will support the State Alliance as it explores different ways to protect the privacy and security of electronic patient information. The Taskforce will provide recommendations to the State Alliance for the development of policies that will address state-level issues related to data sharing.

[28] American Health Information Community (AHIC), information available on the AHIC website at: http://www.hhs.gov/healthit/community/background/.

[29] Apgar, Chris, and Rizk, Stephanie, *Health Information Security and Privacy Collaboration (HISPC) Multi-State Collaborative Issue Brief – DRAFT November 2007*, available at: http://privacysecurity.rti.org/Portals/0/Standards%20Adoption%20Brief.pdf.

Principles, Barriers, and Solutions

The Workgroup identified eight guiding principles they judged were necessary to advance a shared vision that addresses the privacy and security barriers to electronic health information exchange. While many were discussed, Workgroup participants selected the principles that they believed represented the majority of stakeholders' views. In this section, the key principles of accessibility, consumer-centric exchange, emergency access, governance, misuse, security, standards, and sustainability are defined, leading barriers are identified, and specific solutions are proposed that are intended to minimize the impact of the relevant barriers to each guiding principle.

Accessibility

Information is accessible to all stakeholders when appropriate

Workgroup participants agreed that access to electronic data will dramatically change all aspects of care delivery. Today, patient information is largely stored in information silos located at treating provider sites. Duplicating patient information each time a patient visits a provider creates inefficiencies and is a significant driver of the administrative costs that account for approximately 31 percent of total health care spending nationally.[30]

Barriers

Access to data. Paper records and information stored in computer systems that are not interoperable create complex challenges for accessing data. The Workgroup felt that limiting user access to data based on roles is one way to reduce the risk of accidental or intentional misuse of patient information. Role-based access is determined by a set of user profiles that define roles according to responsibilities.

Concerns regarding the use of data. Controlling access to data helps reduce the potential for misuse of patient information. The Workgroup felt that participants must adhere to specified obligations regarding the safekeeping of information before being granted access to data. A HIE with strong privacy and security policies can reduce stakeholder concerns regarding data vulnerability.

Technical and process infrastructure. The Workgroup viewed the lack of policy and an existing infrastructure as an impediment to a statewide HIE. Defining appropriate privacy and security standards requires a consistent understanding among stakeholders regarding federal and state privacy requirements. Some Workgroup participants felt that differences in existing state and federal privacy requirements cause confusion in practices related to disclosure of personal health information.

[30] Woolhandler, Steffie, et al., *Costs of Health Care Administration in the United States and Canada*, The New England Journal of Medicine, 349(*8*), August 21, 2003: p. 2461-2464.

Solutions

Adopt role-based access. The Workgroup agreed that role-based access establishes sound security practices, scales for growth, and requires minimal system administrator support.[31] By controlling user access according to their roles and the attributes attached to those roles, role-based access can provide a HIE with an appropriate control process for managing user access.[32] The user-based identity management method built into many operating systems, and included in several software packages, is problematic in part because as the number of users and applications increases, supporting such a system becomes time-consuming, unwieldy, and expensive.

User authorization was viewed as a high priority by the Workgroup. Identity management has become a critical component in ensuring information security and access control. Implementing role-based access is a complex process for most organizations and requires, among other things, developing a structured work plan that identifies each job function, and defines and analyzes roles to determine appropriate data access levels.

Develop trust agreements. Trust agreements provide the foundation for policies that yield systemic and widespread support for a long term HIE. The Workgroup noted that establishing stakeholder trust presents a challenge to implementing a successful HIE. Trust agreements are an effective way to define standards for data collection, processing, and archiving. Workgroup participants felt that data sharing entities would trust in the security provided by narrowly defined data exchange agreements that outline participant responsibilities and obligations.

The Workgroup believed that trust agreements can provide a mechanism to strengthen the privacy, security, and confidentiality of electronic patient information. Trust agreements must include language that requires participants to conform to existing privacy laws, report to other participants in the HIE when confidentiality breaches occur, create parameters around the acceptable use and disclosure of electronic information, and establish appropriate administrative, physical, and technical safeguards.[33]

Clarify HIPAA and State data sharing requirements. Overly broad interpretation of HIPAA's privacy provision and the lack of familiarity with state requirements often hinder the release of patient information for treatment purposes. Among the issues discussed was the general lack of awareness of the law and frequent misunderstandings that arise as to whether HIPAA allows a certain kind of activity or not, and under what circumstances. HIPAA and state law establish a general rule of confidentiality for health information. Permitted disclosures for treatment, payment, and health care operations are enumerated under HIPAA more explicitly than state law. The Workgroup agreed that further clarification of state and federal laws related to data exchange is needed to ensure that providers are not forced to practice without access to critical information, which can impede quality and contribute to increased costs. Most providers naturally default to HIPAA rather than state law, and although HIPAA was intended to protect patient privacy and promote security and confidentiality of patient information, it has had

[31] Guerin, Trey and Lord, Richard, *Computerworld: How role-based access control can provide security and business benefits*, November 6, 2003.
[32] Ibid.
[33] Markle Foundation, *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, 2005.

unintended consequences for providers. A recent study found more than 70 interpretations of key items in the privacy regulations.[34]

As community and statewide electronic data sharing initiatives develop, the Workgroup felt that stakeholders must implement appropriate policies to safeguard data that are consistent with HIPAA and state law. Balancing stakeholder concerns regarding access to data and protecting data is extremely complex. Stakeholders need to work together to clarify the differences between state and federal privacy provisions to ensure that appropriate measures for accessing and protecting data are deployed.

Consumer-Centric Exchange

Consumers maintain control over the flow of their information
Health information is largely controlled and maintained by the providers who render care and by the insurance companies and other entities that pay for care. The Workgroup agreed that HIE provides a significant opportunity to ensure that consumers control the use of their health information. According to Michael Leavitt, Secretary of HHS, greater use of technology will translate into safer and more efficient care, and will connect more Americans to information on quality and cost.[35]

Barriers

Access to data. Consumers are entitled to access their health records, which is currently scattered among different providers and in formats that are difficult to understand. This makes it challenging for patients to readily access their health information. The Workgroup believed that patients need appropriate access to their data in order to make informed health care decisions.

Concerns regarding use of data. As data sharing begins to mature, consumer acceptance becomes more critical for its success. It is essential to develop an ongoing communication strategy about the potential for data sharing to positively impact care. The Workgroup also noted that a campaign to heighten awareness and educate consumers on the importance of improving the management of their health information could raise concerns regarding the use of data.

Stakeholder trust. Policies and strategies that ensure the appropriate use of data need to be agreed upon in order for electronic patient information to be shared. Secondary data uses pose an interesting challenge to assuring consumers that their data is being used properly. [36] Workgroup participants were inclined to support limited secondary data use in the area of disease management, evaluation of the health care system, and supporting public health and security goals. The Workgroup also felt that consumers require a better understanding on the confidentiality requirement of de-identified data.

[34] Houser, Shannon., et al., *Assessing the Effects of the HIPAA Privacy Rule on Release of Patient Information by Healthcare Facilities*, March 23, 2007.
[35] Leavitt, Michael, *Health IT: Will lead to safer, more efficient care, Leavitt writes*, January 31, 2008.
[36] Safran, Charles, et al., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, Journal of the American Medical Informatics Association, 2007; 14:1-9. DOI 10.1197/jamia.M2273, available at: http://www.jamia.org/cgi/reprint/14/1/1.pdf.

Solutions

Develop a consumer bill of rights. Success of the HIE should not be left to chance. The Workgroup felt that building a foundation of trust by clearly defining consumer rights is critical to realizing the benefits of data sharing and overcoming the pervasive concerns expressed by consumers about unauthorized disclosure and misuse of their health information.

Workgroup participants agreed that consumers should have direct and secure access to their electronic information, except in situations where access to this information could result in harm to the individual or another person. The Workgroup believed that consumers should control whether their information is shared electronically, and should feel secure that the exchange protects the integrity, security, privacy, and confidentiality of their health information.

Establish consumer awareness policies. Exchanging electronic patient information requires a clear, deliberate, and open forum for addressing and settling matters of policy. The Workgroup believed that building consumer awareness is essential to the success of HIE. Consumers should know how to access their information and how to request corrections. They should receive easily understandable information that identifies the entities that can access their information and how their information may be used, shared, or disclosed. This information should clearly identify the intentions for data use, such as for public health, quality improvement, medical research, commercial purposes, or prevention of medical errors.

Developing policies to increase consumer awareness is an effective way to convey the quality and patient safety value that data sharing offers. The more consumers learn about secure data sharing, the more they will embrace electronic health information as a routine part of health care delivery. Workgroup participants felt that consumer awareness policies must, at a minimum, address security, the flow of information, patient permissions, data access, and the benefits to both patients and providers.

Determine a framework for secondary data usage. Consumer concerns regarding secondary data use activities, such as analysis, research, quality and safety measurement, public health, payment, provider certification, accreditation, marketing, etc., are shared by many stakeholders.[37] Determining the appropriate secondary use of data requires ethical, political, technical, and social considerations. The Workgroup agreed that the HIE must ensure that policies are in place to allow for reasonable secondary uses of data. They wanted assurances that under most circumstances that the identities of individuals will be protected. Workgroup participants felt that HIPAA's privacy provisions lack robust safeguards for secondary use of data.

The Workgroup noted the challenge of defining the circumstances for an appropriate release of secondary data. Any decision as to whether identifiable information should be shared with third parties must be in the public interest and carefully evaluated on a case-by-case basis. [38] Workgroup participants believed that such disclosures should be limited to situations where it is essential for preventing a serious and imminent threat to public health or national security, the

[37] Ibid.

[38] Canadian Institutes of Health Research, *Secondary Use of Personal Information in Health Research: Case Studies*. Ottawa, Ontario, November 2, 2002, available at: http://www.cihr-irsc.gc.ca/e/documents/case_studies_nov2002_e.pdf.

life of an individual or third party, or to prevent or detect serious crime. The Workgroup also felt that de-identified data serves a number of purposes and its use can help offset the operating costs of an HIE.

Emergency Access

Rules for emergency access to patient information
When emergency circumstances arise, providers should have the ability to access and view a patient's electronic health information, provided that there is appropriate tracking of such events and subsequent notification to the patient of the occurrence. Typically, patients in distress may not be able to recall critical information contained in their health record. The Workgroup agreed that an HIE must provide access to a core data set and allow for secure and auditable emergency access to patient information.

Barriers

Common patient identifiers. Determining an effective way to identify patients in emergency situations across multiple providers that is flexible, interoperable, and scalable is vital for data sharing. The Workgroup felt that probabilistic matching algorithms provide an accurate, dynamic, and robust way to identify electronic patient information. Probabilistic matching relies on a combination of readily available data, such as name, birth date, zip code, and address, to identify patient information.

Concerns regarding the use of data. Control over one's own confidential information must be balanced against the need for timely data in emergency care situations.[39] The Workgroup agreed that rapid access to patient data in emergent situations is critical to the provision of quality care. Delay of information contributes to substandard and fragmented care, and can be fatal.

Technical and process infrastructure. When designed correctly, HIE has the potential to deliver tremendous returns to patients and providers, particularly those patients requiring emergency care. A data sharing utility should allow authorized users to access select administrative and clinical information in emergency situations. The Workgroup felt that safe, comprehensive, and cost-effective patient care depends on a provider's ability to access a core data set.

Solutions

Establish break-the-glass access policies. The Workgroup agreed that, under certain circumstances, providers need immediate access to patient information. A break-the-glass feature allows providers to view information in emergency situations, and creates an audit log that can be reviewed and validated. The tragedy of Hurricane Katrina demonstrated the need to connect providers and patients with their health information. Thousands of displaced people from the Gulf region were separated from their providers after the disaster. Technology enabled providers throughout the nation to share patient data and provide care to patients that relocated after the storm.

[39] Commission on Systemic Interoperability. *Ending the document game,* 2005, available at: http://endingthedocumentgame.gov/PDFs/entireReport.pdf.

Workgroup participants agreed that a sound infrastructure for data sharing and emergency access policies can significantly bolster access to and use of electronic patient information in the event of disasters. Efforts to implement data sharing following Hurricane Katrina were fairly intense and moderately successful. Under adverse conditions in the months following the storm, the Department of Veterans Affairs found that more than 2,300 users exchanged data electronically across 48 states.[40] If a nationwide infrastructure for data sharing had existed, many more providers would have been able to access patient information electronically.

Develop patient matching algorithm policies. The Workgroup agreed that defined algorithms are required for matching patients to their data in emergency departments (ED). A consistent methodology needs to be developed for emergent situations because of the unique need for rapid access to patient information in the ED. Variability in patient matching algorithms will be fairly common across different organizations. Searches made from a physician's office are likely to be configured with a high threshold, only returning records that are confident matches. This approach reduces the possibility of false-positive matches for searches during routine examinations. In contrast, patient searches performed in the ED will use a slightly lower search threshold to reduce the likelihood of a false-negative (e.g., missed match).[41] Workgroup participants felt that a lower search threshold is necessary in the ED to maximize patient matching opportunities.

The Workgroup noted that it is not just data elements that are important when identifying a patient, but also the matching algorithm used to search and link the available data. Not all probabilistic algorithms are developed using the same criteria, nor will the same algorithm applied to different situations yield identical results.[42] The Workgroup agreed that policies need to be established for determining the elements used in patient matching algorithms for patients in the ED to minimize the rate of false-negatives while simultaneously ensuring the highest possible level of data privacy.

Develop a patient information data set. The Workgroup agreed that a sub-set of data found in paper records that contains the most relevant administrative, demographic, and clinical information about a patient, should be available to all providers. Ideally, this information would provide key summary data that discloses only the information that consumers select to release. Workgroup participants felt that the Continuity of Care Record (CCR) that is under development by ASTM International and several other well-known organizations[43] should act as the source of information to create this data set. The CCR is widely recognized as a transportable set of patient information consisting of the most relevant and timely facts about a patient. The Workgroup considered the patient information data set to be an effective means of providing essential information in emergency situations.

[40] AHIMA e-HIM Workgroup on HIM in Health Information Exchange, *HIM Principles in Health Information Exchange*, Journal of AHIMA 78, no.8, September 2007: online version.

[41] *A recipe for RHIO success and improved patient care, Healthcare White Paper*, Initiate Systems Inc., 2003, available at: http://worldcongress.com/events/nw510/pdf/A%20Proven%20Recipe%20for%20RHIO%20Success.pdf.

[42] Fernandes, Lorraine and O'Connor, Michele, *Future of Patient Identification,* Journal of AHIMA 77(1), January 2006: p. 36-40.

[43] Medical Records Institute, available at: http://www.medrecinst.com/pages/about.asp?id=54.

Workgroup participants felt that the CCR, which contains pertinent information about a patient, provides a suitable framework for the identification of a sub-set of data. This enables the HIE to share a structured data set in a consistent format across participating organizations in urgent situations. Access to data, whether it is limited to a patient information data set or the CCR, will enable providers to analyze trends, put discrete data sets and services into a larger context, and ultimately provide improved diagnostic and therapeutic services.

Governance

The governance body is inclusive and transparent

The governance body must be a transparent, neutral, and sustainable organization that leads efforts to encourage coordination and collaboration, and engages all stakeholders. A public-private partnership facilitates the development of a common framework that enables seamless data exchange among all providers.[44] Workgroup participants agreed that a public-private governance structure is an important component for developing and implementing a shared vision of patient data exchange.

Barriers

Concerns regarding the use of data. The sharing of patient information electronically raises serious concerns about the misuse of data. Concerns about discrimination, the inability to obtain financial loans or insurance, loss of employment, and privacy issues may lead stakeholders to lose confidence in the ability of the HIE to keep information secure. The Workgroup agreed that the governance body must establish robust policies to protect the privacy and security of electronic patient information.

Stakeholder trust. Mistrust presents a difficult, but not insoluble problem in developing trust and recognition between stakeholders. The Workgroup felt that trust will emerge as a result of building stakeholder support for the HIE. A sound governance structure is one that consists of government and private stakeholders, including consumers, and provides the foundation for achieving the mutually beneficial goals of higher quality, safer, and more efficient care.[45] The governance body must have broad stakeholder support and work collectively to establish policies that foster privacy and security.

Technical and process infrastructure. The infrastructure must provide stakeholders with appropriate access to and exchange of information. The Workgroup agreed that the governance body must constantly monitor the latest developments in technology and make the necessary modifications to policy to take advantage of new opportunities. The governance body must continually assess the architecture and the standards used for sharing patient information.[46]

[44] Indiana Center for Urban Policy and the Environment, *Health Information Exchange May Cut Costs and Reduce Medical Errors, but Raise Challenges,* May 2007.

[45] American Health Information Management Association, *Statement on National Healthcare Information Infrastructure,* May 18, 2002, available at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_013733.hcsp?dDocName=bok1_013733.

[46] Ibid.

Solutions

Secure broad stakeholder participation. The Workgroup agreed that broad stakeholder involvement in governance improves the likelihood that the HIE will be sustainable. It also fosters the collaboration necessary to achieve both shared and individual goals. Encouraging stakeholders to participate enables better understanding of their concerns and facilitates development of strategies to manage those concerns. A diverse group of stakeholders ensures that consumer interests are protected, a sustainable business model is developed based on payment programs and incentives, and reliable performance metrics are identified.[47] Workgroup participants agreed that identifying and securing key stakeholder representation is a significant challenge that can impact the success of an HIE.

Selecting representative stakeholders, and establishing and maintaining their broad support, is essential for successful implementation of a statewide exchange. Overall support for exchanging electronic patient information must be garnered from key payers, providers, employers, and purchasers. Early physician involvement and the identification of physician champions are instrumental to promoting acceptance and facilitating support of HIE by physicians and patients.

Build stakeholder trust. Building trust and promoting public accountability are necessary conditions for a successful and sustainable collaboration. The Workgroup felt that the foundation for data sharing relies primarily on trust and goodwill among stakeholders. Current market conditions, payment mechanisms, and a pre-existing environment of competing agendas are not conducive to building stakeholder trust. Workgroup participants agreed that trust builds over time. Other data sharing initiatives have reported that it may take several years for stakeholders to feel comfortable with each other.[48] Outreach and education activities that communicate the positive impact of data sharing are required to achieve the necessary trust, buy-in, and participation of all stakeholders.[49]

Stakeholders will likely have fewer reservations about data sharing if they mutually agree on the governance structure. Ultimately, stakeholders with trust issues will not voluntary participate in sharing patient information electronically.[50] Data sharing is more readily established when trusting relationships are in place, even in the absence of legal guidelines. Stakeholders will only be willing to share data and help pay for up-front and ongoing HIE costs if the sharing of patient information is established through a transparent consensus building process.

Establish a public-private partnership. A successful HIE requires collaboration between the state and the private sector. The Workgroup viewed collaboration as a way to enable learning, enhance networking, and most importantly, overcome the barriers that impede success while

[47] Esterhay, R.J., *Information technology II: health information exchange networks: two regional approaches,* Program and abstracts of the American College of Preventive Medicine Annual Conference; Reno, Nevada. Session 12, February 23, 2006.

[48] Lorenzi, Nancy M., *Strategies for Creating Successful Local Health Information Infrastructure Initiatives,* Vanderbilt University, Department of Biomedical Informatics, December 16, 2003.

[49] The American Health Quality Foundation, *Quality Improvement Organizations and Health Information Exchange,* March 6, 2006: p.22, available at: http://www.ahqa.org/pub/uploads/QIO_HIE_Final_Report_March_6_2006.pdf.

[50] Malepati, Sarath, Kushner, Kathryn, and Lee, Jason S., *RHIOs and the Value Proposition: Value Is in the Eye of the Beholder*, Journal of AHIMA, March 2007: p. 24-29.

managing the organizational, financial, legal, technical, and practice transformation challenges.[51] Many early data sharing initiatives were negatively impacted due to the inability of stakeholders to access information or have a reliable way to exchange data. The Workgroup believed that a public-private partnership can identify and facilitate the development of appropriate policy and, if necessary, legislation that may be required to improve the privacy, security, reporting capabilities, and management of electronic patient information.

The American Health Information Management Association has called for privacy legislation to make certain that all individuals can be assured that their personal health information is protected from intentional misuse in whatever form it resides or wherever it is collected, utilized, transferred, or rests.[52] Workgroup participants viewed state and private collaboration as an effective way to identify essential privacy and security policies, and as an instrumental vehicle for implementing a transparent and publicly accountable governance structure.

Misuse

Specific formal penalties exist for the misuse of patient information
The intentional and unwarranted access to, use of, or distribution of electronic patient information for nefarious purposes must be prevented. While data sharing holds many potential benefits for consumers, it raises serious concerns about the potential misuse of patient information. The Workgroup agreed that the enormous benefits of interoperable data will not be realized unless appropriate policy measures are established to mitigate consumer concerns.

Barriers

Concerns regarding the use of data. Concerns regarding the privacy and security of health information are escalating, owing both to the growing use of HIT and to increasing consumers' demand to control the use of their information.[53] Advances in HIT have contributed to consumers' concerns about safeguarding the use of their health information. Consumer fears have caused some patients to withhold important information, which can result in individual care and public health data being compromised. The Workgroup viewed safeguarding data as essential to ensuring that patients are comfortable enough to communicate honestly and openly with their providers.

Liability. Health information differs from other personal data because it is more private, intimate, and sensitive; as such, it warrants greater protections. Inappropriate use and disclosure of patient information can result in considerable liability for HIE participants that is not easily remedied. Provider anxiety about the liability associated with the use of data that they disclose increases their reluctance to participate in data sharing. The Workgroup did not view the safeguarding of information as a technology matter; rather, they viewed it as a policy matter which, if not addressed, could stall efforts to improve patient safety using technology.

[51] eHealth Initiative Foundation Report, *Health Information Exchange: From Start up to Sustainability Frequently Asked Questions*, June 5, 2007.
[52] American Health Information Management Association, *Statement on the Confidentiality, Privacy, and Security of Health Records Approved*, December 2007, available at*:* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_036103.hcsp?dDocName=bok1_036103.
[53] Kirshen, AJ, and Ho, C. *Ethical considerations in sharing personal information on computer data sets.* Canadian Family Physician, 1999; 45:2563–2565, 2575-2577.

Stakeholder Trust. Building a network of trust is an essential prerequisite for sharing electronic patient information. Stakeholders' willingness to trust their competitors and not fear that data will be misused is pivotal to a statewide exchange. The Workgroup believed that providers must be willing to exchange a sufficient amount of clinical data in order for HIE to provide value to all stakeholders.

Solutions

Implement technical safeguards. Many stakeholders are concerned about determining the appropriate level of safeguards that are needed to secure their data. The Workgroup agreed that technology must be secure, protect confidentiality, and make information easily accessible to appropriate parties. Open standards and interfaces enable additional layers of protection using strategies such as data classification, identity management, and encryption.[54] When data is not appropriately secured, there is virtually no assurance that data access, use, or modification follows established policy. Workgroup participants agreed that implementing appropriate safeguards reduces the possibility for misuse and ensures that the right data can be accessed by the right people, at the right time, and for the right reasons. Appropriate safeguards can simplify access for the right people, while making access by the wrong people cumbersome, expensive, and easily detected.

The Workgroup viewed robust technical safeguards as necessary to protect consumer interests against inappropriate access to their health data. Consumer concerns are not limited to the transmission of data, but also arise from fears of intrusion into the HIE and non-health related information being accessed and used for commercial or criminal purposes.[55] Patient information is regarded as private, particularly when it contains information regarding sensitive health conditions.[56] Unauthorized access to electronic health information has already occurred, both locally and nationally. The Workgroup viewed establishing strong safeguards as a critical activity for data sharing.

Develop consumer-managed audit reports. Nearly all consumers are concerned about the privacy of electronic health information. Concerns are extensive and range from misuse during treatment to secondary use of the data. Misuse of health information can lead to discrimination, stigmatization, or loss of insurance or employment.[57] The Workgroup believed that consumers should have the ability to know who has viewed their health information. Consumer-managed audit reports should enable ad hoc review of entities that have entered, accessed, modified, and/or transmitted any of their health information. Misuse of data creates participant liability and generates negative publicity, which may jeopardize the credibility of HIE. Audit reports will assist in identifying those individuals responsible for privacy breaches.

[54] Sun Microsystems, Inc., *Engineering for Data Protection and Accountability*, *A Technical Whitepaper*, May 2007, available at: http://www.sun.com/software/products/identity/wp_eng_data_protection_accountability.pdf.
[55] National Research Council, *For the record: protecting electronic health information*, Washington, DC: National Academy Press; 1997.
[56] Pieper, M. and Stroetmann, K., *Patients and EHRs tele home monitoring reference scenario*, Stephanidis, C. ed. *Universal access code of practice in health telematics*. Berlin/Heidelberg: Springer Verlag; 2005: p. 77–87.
[57] Kulynych, J. and Korn, D., *The Effect of the New Federal Medical-Privacy Rule on Research*, The New England Journal of Medicine, January 17, 2002.

Consumer-controlled audit reports will curb misuse of data and ensure accountability by maintaining a record of who has accessed data. Workgroup participants felt that standard audit reports should include, at a minimum, the individual accessing the data, the information accessed, the date and time of access, and all failed attempts to access data. Consumers need to know that a process is in place to alert the HIE that information may have been inappropriately accessed.

Develop data sharing agreements. Data sharing agreements facilitate intrastate HIE while addressing concerns related to privacy and security. The Workgroup viewed formal agreements among participants as a requirement for participating in a statewide data exchange. In general, data sharing agreements serve as the cornerstone for the relationship between often highly competitive stakeholders. They establish consistent rules and foster the development of complex relationships, consensus building activities, and the deliberation process for a successful HIE.[58] Workgroup participants felt that data sharing agreements provide a mechanism for entities to train staff regarding the confidentially of patient data, and ensure that staff understands that breaches of confidentiality may result in exclusion from the HIE.

Data sharing agreements are a means to promote cooperation by defining the data that can be shared, and the circumstances for data sharing between HIE participants. As the number of stakeholders sharing data increases, it is important that measures are in place to protect the privacy and security of health information. Data sharing agreements serve as the foundation for structured data sharing relationships by defining the authorized uses and disclosures of the data, providing for a participatory management structure, ensuring compliance with applicable laws, and offering some participant protection from liability, should unforeseen events occur.[59]

Security

Data security protects patient privacy
Establishing strong safeguards for electronic health information is essential to ensuring the sustainability of an HIE. The Workgroup agreed that rigorous security standards need to be adopted to reduce the risk that patient information will be vulnerable to modification, loss, or theft. System functionality, user training, and security monitoring are all predicated on establishing well-defined parameters for securing access to data.

Barriers

Access to data. Keeping patient information secure is critical to building stakeholder acceptance of electronic health information, while facilitating appropriate access at the point of care. Comprehensive information about patients is frequently unavailable when care is delivered. The Workgroup agreed that policy must enable consistent access to data in order for providers to deliver quality care.

Concerns regarding the use of data. Developing policies aimed at protecting the use of data within an HIE presents enormous challenges. When electronic patient information is exchanged,

[58] Information Management for State Health Officials, *Privacy Issues in Public Health Information Exchange Across State Lines,* 2006, available at: http://www.astho.org/pubs/StatetoStateIssueRpt.pdf.
[59] Sears, Christopher S., Prescott, Victoria M., and McDonald, Clement J., *The Indiana Network for Patient Care: A Case Study of a Successful Healthcare Data Sharing Agreement*, 2005.

it can be unknowingly corrupted when it transfers through a data sharing utility, affecting both the sender and the receiver of the information. Workgroup participants believed that data integrity can be assured through the establishment of robust security policies.

Technical and process infrastructure. The prospect of storing, moving, and sharing patient information electronically presents new challenges for ensuring strong data security. The lack of uniform standards and data protections hinders interoperability. The Workgroup agreed that establishing guidelines for performing routine and non-routine audits would provide the necessary protections for ensuring that patient information is protected.

Solutions

Establish data sharing control policies. Ensuring data security is a significant challenge to sharing electronic data between disparate systems, especially when connecting to the Internet. Rigorous data sharing control policies must be established before any data is exchanged.[60] The Workgroup agreed that stakeholders should implement a broad range of control policies that include, but are not limited to, accountability, access, data integrity, non-repudiation, and availability. The Workgroup felt that the HIE needs to find the right balance between stringent security controls and ease of data sharing.

While it is crucial that data communications be highly secure and protective of patient privacy, a pragmatic approach to information security dictates that the technology requirements not be so complex that they inhibit growth of the HIE.[61] Exchanging patient information electronically requires stakeholders to trust the data and incorporate controls to verify that a violation of that trust has not occurred. The Workgroup felt that an HIE should monitor whether trust has been violated, identify the person violating that trust, and link that person unambiguously to the entity that provided access to the information.

Identify critical data integrity assurance activities. New security vulnerabilities will arise as patient information is increasingly stored and transmitted electronically. The Workgroup agreed that appropriate assurance mechanisms create higher confidence in the data that is stored and exchanged. Network protocols need to be identified and agreed upon to make sure that the data transmitted is the same as the data received. The Workgroup noted that alleviating concerns regarding data sharing requires stakeholders to identify and implement appropriate integrity assurance activities, such as penetration testing, code auditing and analysis, and specific hardware and software security controls. When undetected, minor integrity violations can harm data, and may cause even more serious problems than confidentiality breaches. Integrity violations can occur because of hardware or software malfunctioning, malicious intrusion, or inadvertent user error.[62]

[60] IHE IT Infrastructure, *White Paper: HIE Security and Privacy through IHE,* August 15, 2007, available at: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Whitepaper_Security_and_Privacy_2007_07_18.pdf.).
[61] Markle Foundation, *P5 – Authentication of System Users, Connecting for Health,* April 2006: p. 3-4.
[62]Barlett, W. and Spainbower, L., *Commercial fault tolerance: A tale of two systems. In Proceedings of the IEEE Transactions on Dependable and Secure Computing*, January 2004: p. 87-96.

Workgroup participants also felt that establishing integrity assurance activities for edge systems could minimize the potential for data to become corrupted. These activities are all built on a set of assumptions that are generally applied in conjunction with overall risk management goals.[63]

Establish security audit guidelines. Security audits are required to ensure that data is used for intended purposes and access to data is not misused. The Workgroup agreed that an HIE security audit process does not need to be exhaustive, but should attempt to investigate the compliance level of all participants. Security audits provide a reasonable back-end glimpse at system and policy effectiveness for protecting data.[64] Audit information may also be useful during security investigations into incidents of possible violations. The Workgroup remarked that audits do not eliminate threats to security; rather, they can generate substantial benefits by mitigating risks and building stakeholder confidence in the exchange.

Data sharing requires a fairly complex security audit management system that reviews and analyzes information. Security audits use audit trails and audit logs to compare actual system activity to expected activity. In general, an audit trail consists of log records that identify a particular transaction or event, whereas audit logs are used to compare actual activity to expected activity. The audit process reviews both the audit trail and audit log to identify discrepancies. Workgroup participants believed that stakeholders need to reach consensus on what data must be logged for security and operational considerations. Stakeholders will need to determine how long audit information should be retained, how it will be destroyed, who should have access to it, who will be responsible for reviewing it, and the frequency of review.

Standards

Information exchange standards are agreed upon and in use

Harmonizing standards around data content and technology enables data to flow between disparate systems. While a number of technical and messaging standards have been defined for exchanging patient information, universal standards have not been adopted. The Workgroup felt that variation in adopting existing standards will inevitably impact the ability to maximize data sharing. Uniform standards are required for interoperability, particularly in the areas of patient matching and data exchange.[65]

Barriers

Access to data. Significant consumer concern exists regarding access to sensitive information through an HIE. The Workgroup agreed that access to electronic information must be carefully granted and limited to necessary and authorized instances for disclosure. Technology needs to allow patients to control the flow of their information so they can decide how their information is viewed, stored, and accessed.

Common patient identifier. Patient identifiers are used to uniquely identify a patient for care and administrative activities. The same patient can acquire multiple identifiers from both the

[63] Peterson, Gunnar: *Security Architecture Blueprint*, Artec Group LLC, 2006 & 2007.
available at: http://www.arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf.

[64] Hjort, Beth. *AHIMA Practice Brief: Security Audits*, November 2003.

[65] AHIMA e-HIM Workgroup on HIM in Health Information Exchange. *HIM Principles in Health Information Exchange*, Journal of AHIMA 78(8), September 2007: online version.

same and different providers and, conversely, multiple patients can be accidentally assigned the same health record number. The Workgroup agreed that the issue of patient identifiers must be resolved in order for HIE to succeed.

Technical and process infrastructure. An HIE must agree on processes that facilitate information sharing among stakeholders. The Workgroup felt that the infrastructure should be built to support agreed-upon standards. All stakeholders must adopt consistent standards in order to exchange patient information. While several data and messaging standards have been defined, a single universal set of standards is not currently in place.

Solutions

Identify standards and develop implementation guidelines. A statewide HIE should demonstrate a commitment to implementing standards and clearly defining the approach for implementation of those standards. All stakeholders must have a clear definition and understanding of the standards. Presently, many systems are incapable of generating standard electronic messages or cannot format data in conformance with national standards. The Workgroup noted that disparate systems will require additional technology to integrate standards in a way that will allow them to interpret data. Identifying which standards and versions should be used by an HIE, and developing guidance on implementing the standards, assures consistent electronic messaging between disparate systems. The Workgroup agreed that stakeholders will require strong guidance to appropriately implement standards.

Standard development organizations involved in data sharing include Health Level Seven, ASTM International, the Accredited Standards Committee X12, and the National Council for Prescription Drug Programs. The National Committee on Vital and Health Statistics (NCVHS) serves as a council to these voluntary industry efforts.[66] In addition to these data standard groups, other similar public and private groups exist for the development and maintenance of standards for terminologies and classifications.

Establish guidelines for storing data in an Enterprise Master Patient Index. Accessing organization-wide electronic patient information requires a consistent methodology for retrieving information. An Enterprise Master Patient Index (EMPI) is a database that contains unique identifiers for every patient seen by a provider within an organization with multiple sites. An EMPI typically uses deterministic indexing where searches are based on an exact match of select demographic information.[67] The Workgroup agreed that an established framework for defining data elements for an EMPI reduces design complexities of a Record Locator Service (RLS), which is a patient information system that creates pointers to the locations of patient records.

HIPAA recognized unique individual identifiers as an essential component of administrative simplification. NCVHS was given a special role by HIPAA to advise the Secretary of HHS on standards issues. They recommended that HHS not adopt standards for unique individual identifiers until strong privacy legislation is enacted. Although mandated by HIPAA, Congress

[66] Rode, Dan, *Connecting the Dots: Outlining the Organizations Involved with EHRs and HIE,* Journal of AHIMA 78(4), April 2007: p. 18-20.

[67] American Health Information Management Association, *MPI Task Force: Practice Brief*: *Maintenance of Master Patient (Person) Index (MPI*) -- *Single Site or Enterprise*, October 2005, available at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_000071.hcsp?dDocName=bok1_000071.

has adopted budget language to ensure no such standard is adopted without congressional approval.[68]

Determine design complexity of a Record Locator Service. A RLS is a key infrastructure component that supports interoperability in a decentralized data exchange environment. The RLS provides directory and registration services for data sharing, primarily through a user-defined index of pointers to the location of patient information.[69] The combination of EMPI access and interface message tracking supplies the necessary technical elements to develop an RLS. Stakeholders need to agree on the complexity of the algorithm that will be used by the RLS to validate patient records across providers. The Workgroup felt that using probabilistic demographic matching techniques would ensure the privacy and security protections of patient records.

Workgroup participants noted that an HIE must define probabilistic matching algorithms in such a way as to keep the positive match threshold set high enough to reduce the likelihood of false-positives to negligible levels. Establishing a balance between privacy and security is a key issue for consideration in determining the complexity of an RLS.

Sustainability

A well defined value proposition and equitable business model

The key to sustainability is working with stakeholders to identify and develop a business model that meets the needs of stakeholders and is diverse enough to accommodate future changes. The Workgroup felt that identifying a value proposition and a viable funding mechanism that is equitable to all stakeholders is a significant challenge. Addressing issues related to cost sharing, technology adoption, and privacy and security is required before stakeholders will participate in an HIE.

Barriers

Funding. It is important to understand the degree of stakeholder willingness to participate in different types of data exchange activities, as well as the level of participation that they can support. To achieve sustainability, providers must contribute enough clinical data to make sharing information valuable to the participants.[70] Stakeholders must be willing to invest in the operations through a subscription model, a transaction-based model, or some combination thereof. Workgroup participants agreed that the highly competitive nature of health care sometimes contradicts the goal of sharing patient information.

Interoperability. The ability to exchange information, and have the meaning of that information automatically interpreted by the receiving system, is seen as the most critical element to effective data sharing. The Workgroup agreed that the ability to synthesize all of a

[68] National Committee on Vital and Health Statistics, *Second Annual Report to the Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act, Executive Summary,* available at: http://www.ncvhs.hhs.gov/yr2-sum.htm.

[69] *The Connecting for Health Common Framework, T6 Record Locator Service,* October 2006.

[70] Grossman, Joy M., Kushner, Kathryn L., and November, Elizabeth A., *Creating Sustainable Local Health Information Exchanges: Can Barriers to Stakeholder Participation be Overcome?* Research Brief No. 2, February 2008.

patient's information into a single view that provides accurate and current information at the point of care remains a sizable challenge. This challenge can be solved by technology, but requires adequate privacy and security protections.

Liability. Concerns related to electronic clinical information primarily revolve around who will be held accountable for the content of the information exchanged, inappropriate disclosures, medical malpractice, and the obligation to verify sources of information. The Workgroup agreed that a significant barrier to HIE is the issue of assigning responsibility for the inappropriate transmission of data or the content of the information provided.

Solutions

Identify benefits unique to each stakeholder. Developing a sustainable business model that provides value for all stakeholders is necessary for a HIE to succeed. In the early stages of developing an exchange, most of the value will be intangible and primarily focus on improving health care quality.[71] Stakeholders must address the differing perspectives and needs of each participant, while recognizing that data sharing requires enormous cooperation. The experience of sustainable data sharing models suggests that each began with stakeholders identifying the functions of highest value to them.[72] Clearly defining value helps guide efforts to develop a funding model, which will likely consist of some combination of user fees and subscription costs.

The Workgroup believed that value will be defined on a continual basis as small, incremental steps are taken in the construction of a data sharing application. An incremental approach also allows for the flexibility to add features at an acceptable pace.[73] Workgroup participants favored an incremental approach that develops key sustainable data sharing services in a logical stepwise fashion, is consensus driven, and value-based.

Implement a Service Oriented Architecture. A Service-Oriented Architecture (SOA) is a design approach that guides how the exchange should be built. The purpose is to organize distributed systems into an integrated approach that eliminates information silos. Workgroup participants noted that most successful data sharing models have adopted an SOA. The SOA does not require re-engineering of existing systems. Instead, it supports existing functionality by loosely connecting systems to integrate information across systems.[74] SOA enables systems to interoperate using Internet-based protocols that can have a dramatic impact on cost by preserving and extending the use of existing systems.[75]

[71] Deloitte Center for Health Solutions, *Health Information Exchange (HIE) Business Models, The Path to Sustainable Financial Success*, 2006.

[72] Michigan Health Information Network Resource Center, *Health Information Exchange: Basic Functions and Stakeholder Value*, January 2008, available at: http://www.mihin.org/resources/HIE_Value_Propositions.pdf.

[73] Modified from HIMSS-EHR Vendors Association Interoperability Roadmap, available at: http://www.himssehrva.org.

[74] Juneja, Girish, Dournaee, Blake, Natoli, Joe and Birkel, Steve, *Service Oriented Architecture Demystified*: *Improving Performance of Healthcare Systems with Service Oriented Architecture*, available at: http://www.intel.com/intelpress/sum_soa.htm.

[75] Sun Microsystems, Inc., *Implementing Health Information Technology for RHIO Success, White Paper*, September 2005, available at: http://www.sun.com/software/whitepapers/integration_suite/rhio_healthercare_wp.pdf.

The Workgroup believed that the evolution of data sharing depends on effectively integrating existing legacy systems. SOA architecture promotes efficiency in data transmission through a well-designed system integration scheme. SOA enables participants to design a solution that represents a dynamic collaboration of applications.

Include Safe Harbors in trust agreements. Uncertainties about the potential risks in sharing data have posed significant barriers to widespread adoption of an HIE. Safe Harbor language is intended to address the challenge of unknown liability and provide appropriate measures to mitigate risks to stakeholders.[76] The Workgroup recommended including Safe Harbor language, comparable to hold harmless clauses, in trust agreements. The basic premise of Safe Harbor language is to foster industry self-regulation. Workgroup participants felt that stakeholders could agree at some level on self-regulation as a meaningful way to mitigate liability concerns. Participants must demonstrate a willingness to ensure that appropriate data sharing protections and sanctions for violations are in place in order for self-regulation to be a convincing alternative to legislation.

Data sharing will not occur if stakeholders have unresolved liability concerns.[77] Stakeholders need to be confident that an HIE has adequately addressed privacy and security issues and minimized their risk of liability. The Workgroup agreed that concerns about liability for incidental or inappropriate disclosures deter participation in HIE. Including Safe Harbor language in trust agreements can mitigate those concerns.

[76] Redhead, C. Stephen, *Health Information Technology: Promoting Electronic Connectivity in Healthcare*, CRS Report for Congress, Life Sciences Domestic Social Policy Division, April 13, 2005.

[77] Dimitropoulos, Linda L., *Privacy and Security Solutions for Interoperable Health Information Exchange, Nationwide Summary*, Prepared for: Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services, RTI Project Number: 0209825.000.009, July 2007.

Implementation Activities

The Workgroup carefully considered the privacy and security barriers that impact HIE and, using the guiding principles identified previously in this report as a foundation, identified the implementation activities (activities) contained in this section. Workgroup participants felt that these activities could be used to craft detailed work plans to overcome the barriers to HIE. These activities are not intended to be all inclusive; instead, they target what the Workgroup felt were critical barriers to HIE implementation.

Accessibility

Adopt role-based access

- Determine data access parameters for each role identified, taking into consideration the needs of emergency care delivery staff.
- Establish guidelines that require access based on position classification, such as physician, nurse, administration, secretary, nursing assistant, etc.
- Identify a user credentialing mechanism for establishing and maintaining system access.

Clarify HIPAA and State data sharing requirements

- Assess the effects of current privacy business practices for each Sector Group.
- Identify key privacy and security policies for data sharing that are consistent with suitable business practices, and state and federal laws.

Develop trust agreements

- Define the circumstances for entering into a trust agreement.
- Determine components for inclusion in trust agreements that address the appropriate uses of electronic patient information, rules for data exchange, and privacy and security requirements.
- Identify which entities and participants are required to enter into trust agreements.

Consumer-Centric Exchange

Determine a framework for secondary data usage

- Develop guidelines for using secondary data and define the elements of a valid data usage agreement.
- Develop policies for de-identification and pseudo-anonymization of data.
- Identify permissible secondary uses beyond those for biosurveillance and public health purposes.

Develop a consumer bill of rights

- Determine the fundamental components of a consumer bill of rights that includes among other things, whether participation is on an opt-in or opt-out basis, consumer controls, access guidelines, information disclosure, confidentiality, complaints and appeals, and consumer responsibilities.

Establish consumer awareness policies

- Develop a consumer awareness outreach strategy that determines how information is disseminated and the mechanisms for outreach.
- Establish a process for updating consumers regarding changes to HIE policies and business practices.
- Identify the components of consumer awareness policies, which should include security, the flow and use of information, patient permissions, data access, and the benefits for data sharing.

Emergency Access

Develop a patient information data set

- Identify the key elements of a paper record that includes name, address, age, gender, allergies, current medications, etc.
- Develop guidelines for the use of the data set.
- Develop parameters for creating, accessing, and maintaining the data set.

Develop patient matching algorithm policies

- Determine the key data elements that should be included in patient matching algorithms.
- Establish rules to validate patients’ identity with respect to their EHR.
- Identify acceptable parameters for determining patient identification that will minimize the number of false-positive or false-negative results.

Establish break-the-glass access policies

- Develop an audit policy that tracks user access and mitigates system infractions.
- Establish a consumer notification policy for alerting individuals when their data has been accessed.
- Identify the criteria for granting emergency access that includes who has access, the circumstances allowing access, and patient consent requirements.

Governance

Build stakeholder trust

- Determine a consistent, reliable, and transparent process for stakeholder communication.
- Identify the business and technical policy categories for building a transparent HIE.

Establish a public-private partnership

- Establish a process for determining an appropriate business configuration.
- Identify the rules of governance that include how stakeholders will govern the HIE as an organization.
- Develop mission and vision statements that convey goals and objectives.

Secure broad stakeholder participation

- Identify individuals from each stakeholder group to participate on the governing body.

Misuse

Develop consumer-managed audit reports

- Create a process that notifies consumers when their data has been accessed.
- Define the data elements for audit reporting, which should include a date/time stamp, identification of the person accessing the record, and the data accessed.
- Establish a process for consumers to report suspected inappropriate use of their information.

Develop data sharing agreements

- Determine which organizations and individuals are required to enter into data sharing agreements.
- Identify the components for data sharing agreements, including appropriate privacy and security requirements.

Implement technical safeguards

- Define the policies that will protect data from inappropriate use and disclosure.
- Determine the frequency for reviewing the policies related to technical safeguards.
- Identify the technical safeguards needed to reduce the risk of inappropriate data access.

Security

Establish data sharing control policies

- Develop data sharing control policies to ensure that security standards are adequate to protect electronic health information.
- Develop stringent sanction policies to deter inappropriate access, use, and disclosure of patient information.

Establish security audit policies

- Develop audit guidelines to ensure that appropriate protections are in place.
- Identify the key data elements that should be included in a security audit.

Identify critical data integrity assurance activities

- Establish appropriate mechanisms to ensure that stored or transmitted data is unchanged from its original data source.
- Identify a method to assess data integrity risks and remediate weaknesses.

Standards

Determine design complexity of a Record Locator Service

- Determine the key data elements that should be included in an RLS.
- Establish a core set of parameters for the algorithm that will be used by the RLS.
- Identify minimum threshold criteria for positive patient matching that minimizes false-positive or false-negative results.

Establish guidelines for storing data in an Enterprise Master Patient Index

- Define the key data elements that should be included in an EMPI.
- Determine critical policies needed to maintain the ongoing accuracy of the EMPI.

Identify standards and develop implementation guidelines

- Develop a process to evaluate and implement the standards adopted by the governance body.

Sustainability

Identify benefits unique to each stakeholder

- Determine leading benefits for stakeholder participation in the HIE.

- Develop a communication strategy to regularly update stakeholders about the successes and challenges of data sharing.

Implement a Service-Oriented Architecture

- Develop a technology evaluation guide for organizations with multiple legacy systems to use in determining a logical grouping of these systems.

Include Safe Harbors in trust agreements

- Evaluate Safe Harbor language for inclusion in trust agreements.
- Establish a policy to review and update Safe Harbors in trust agreements.

Desired Future State

One of the most significant tasks in developing an HIE is to foster a shared vision among stakeholders and develop a strategy for achieving the desired future state. The Workgroup felt that each of the principles they identified are interconnected and achievable with a coordinated effort by all stakeholders. The desired future state is intended to act as a catalyst for stakeholders to work collectively to ensure that electronic patient information is available for all Marylanders whenever and wherever care is provided throughout the state. The following section provides an overview of the guiding principles for a future state.

Accessibility

An environment exists where all stakeholders have the ability to access a predetermined amount of electronic health information, and consumers control access to their health information. Secure access exists for all participants, and sound policy is established to safeguard information. Providers rendering patient care have real-time access to a limited amount of data during the treatment process, with additional data available upon patient approval. Consumers can track who has viewed their data and have a mechanism for resolving disputes regarding unauthorized access. The secondary use of data is clearly defined, and specific information is routinely used for public health purposes, biosurveillance activities, conducting clinical research, measuring performance, assessing quality, and improving population health.

Consumer-Centric Exchange

Consumers are empowered to participate in the HIE and control who has access to their information, limit what information can be viewed, and make informed decisions about their health care. Consumers are integral and active participants in HIE governance decisions regarding privacy and security policies. The HIE enables consumers to actively monitor and manage their health status. The HIE supports private and secure patient communication with providers, allowing them to receive medical consultations from home, schedule appointments, track immunizations, or request prescription refills. Consumers are able to participate in health education, wellness, and prevention programs through the HIE.

Emergency Access

Providers and public health officials are able to rapidly access patient information in emergency situations. In a situation where a patient is unable to grant access to their information, break-the-glass rules clearly define what constitutes an emergency, what data is accessible, and what entities or individuals are able to access patient information, with access dependent on the role of the individual or entity using the data. National standards have been developed and provide a framework for emergency access policies that allow access to information across state boundaries. Consumers are informed whenever their information is accessed, and regularly scheduled back-end audits are performed to ensure that access is appropriate and patient information has not been compromised. Patients are accurately identified and matched to their data and providers are able to treat patients when there is no previous relationship, particularly in the event of a natural disaster or catastrophe.

Governance

A public-private partnership collaborates synergistically to ensure that all the goals of the governance body are achieved and maintained. Participants on the governance body represent the diverse needs of all stakeholders. Comprehensive privacy and security policies and procedures exist with penalties for misuse clearly defined. The governance body upholds standards and protocols for the exchange of data, enabling effective statewide exchange of patient information and allowing for interstate data sharing. A mechanism exists for harmonizing data exchange policies within the state to ensure that local policies are consistent with national policies. The statewide exchange is built upon the trust of the health care community and residents throughout Maryland. The HIE is self-sustaining, has improved the quality of health care in the state, and provides an array of services that meet the health information needs of providers, consumers, and public health entities.

Misuse

Sound privacy and security protections exist to ensure that misuse of patient information does not occur. Robust technological safeguards are in place. If unauthorized access to patient information occurs, security alerts are immediately generated. Comprehensive audit information is available, and user-friendly reports are generated and reviewed on a regularly scheduled basis. Consumers are electronically alerted when their information is inappropriately accessed. Consequences for the intentional misuse of data are clearly defined and conform to national penalties. Data sharing agreements protect exchange participants from liability resulting from the misuse of electronic patient information. Consumers are confident that the safeguards established by the exchange protect their health information.

Security

Security risks are mitigated through periodic risk assessments that include review of security policies, procedures, and data encryption standards and techniques. Basic security functions are defined and include audit trail requirements and node authentication profiles to ensure that the HIE will accurately authenticate the edge systems, and only trusted systems are able to access the HIE. The HIE is able to provide a rapid and appropriate response to new and more destructive viruses or malicious intrusion techniques. For example, biometric authentication, such as fingerprints or retinal scans, is the standard and required method of authentication for accessing electronic patient information. Business continuity and disaster recovery plans are developed, fully tested on a regularly scheduled basis, and a hot site is established to ensure that the exchange of patient data is not hindered in the event of a disaster.

Standards

Standards that provide for the private, secure, and interoperable exchange of electronic health information are employed. These standards are aligned with national standards, enabling the

HIE to participate in the Nationwide Health Information Network. Exchange participants comply with a defined set of privacy and security standards that foster patient awareness of how their information is used and disclosed, and have been adopted by all stakeholders. Technical standards that facilitate interoperability are harmonized, including standards for data content, data formats, and data exchange. These standards are continuously assessed to ensure that they comply with nationally recognized standards. Standards for EHR data quality metrics are prevalent, and providers are able to generate standard reports that can be shared electronically.

Sustainability

The HIE has a sustainable business model that provides value to its participants and generates adequate revenue to maintain ongoing operations in a private and secure environment. The model is designed to minimize the need for public funding and grants. The exchange has sufficient financial resources for service enhancements, new and revised data and exchange standards, and accommodates improvements and changes in technology. Participant cost is proportionally aligned with the benefits derived from the exchange. The HIE demonstrates value by meeting the needs of participants, improving health care quality and outcomes, reducing the costs of health care, and enhancing public health activities. Participation in the exchange is not hampered by competitive fears because the HIE has succeeded in demonstrating its value to the state and has earned the trust of its participants.

Looking Ahead

Results from the Workgroup's effort to identify privacy and security barriers related to HIE will be used in developing detailed work plans that address these barriers. This work is part of a process intended to further dialogue among stakeholders regarding appropriate policies for the private and secure exchange of electronic health information in Maryland. The information obtained in this report will further guide the planning and implementation efforts of a statewide HIE. Continued stakeholder input is essential to identifying an appropriate infrastructure to support information sharing. Collaboration among stakeholders ensures that local data sharing needs are appropriately addressed while helping to evaluate policies against national HIE efforts.

The collaboration of the Workgroup has helped to build trust among all of the stakeholders. As a result of this effort and other initiatives, stakeholders are becoming increasingly excited about the potential for data sharing, seeing the many benefits and functioning more collegially in their efforts to resolve the barriers that must be addressed before significant progress can be made in data sharing. The collaborative effort by the Workgroup has aided in building a framework for the advancement of a private and secure HIE in Maryland.

Acknowledgements

MHCC greatly appreciates the contribution made by everyone that participated in the Workgroup meetings, and to those individuals that provided ongoing support to the project during the data analysis and report writing phase. This report was made possible due to the hard work and dedication by the staff of the Center for Health Information Technology. MHCC also thanks Mosaica Partners for facilitating the Workgroup meetings.

Appendix A

Solutions and Implementation Participant List

(Participant information based on December 2007 data)

Douglas A. Abel, MBA
Chief Information Officer
Anne Arundel Medical Center

Lynn Albizo, Esq.
Executive Director
National Alliance on Mental Illness

Salliann Alborn
Chief Executive Officer
Community Health Integrated Partnership

Marcia Behlert
Director of Benefits
Constellation Energy Group

John Bernas
Manager, Integration Services
MedStar Health

Meryl Bloomrosen
Associate Vice President
American Medical Informatics Association

Shirley Brown-Ornish, M.D.
Physician
Prince George's Health Department

Jon P. Burns
Senior Vice President &
Chief Information Officer
University of Maryland Medical System

Cathy Casagrande, R.N.
Privacy Officer
Frederick Memorial Health System

Beverly Collins, M.D., MBA
Medical Director, HC Informatics
CareFirst

Rex W. Cowdry, M.D.
Executive Director
Maryland Health Care Commission

Gretchen Derewicz
Director, State Mission Delivery
American Cancer Society

Damien Doyle, M.D.
Director, Outpatient Services
Hebrew Home of Greater Washington

Carol Emerson, M.D.
Physician
St. Agnes OB/GYN Associates

Michaeline R. Fedder, MA
Advocacy Director, Maryland
American Heart Association of Maryland

Irwin Feuerstein, M.D.
Radiologist
National Institutes of Health

Mike Fierro
Associate Vice President for
Healthcare Informatics
CareFirst

Carla Flaim
Director, Management Information Systems
Healthcare for the Homeless

Richard Fornadel, M.D.
Medical Director
Aetna

Sheila Frank
Director, Health Information Standards
Delta Dental Plans Association

Eileen Giardina
Vice President, Quality Management and
Preventative Health
United Healthcare Mid-Atlantic

John Gutwald
Assistant Vice President
MedStar Health

Terry Hardcastle
Vice President
Primary Care Coalition

Charles Henck
Chief Information Officer
University Physicians, Inc.

Mary Jean Herron
Chief Financial Officer
Healthcare for the Homeless

Jeff Huddleston
Senior Director, Information Technology
University of Maryland Medical System

Patricia Rutley-Johnson
Senior Staff Advisor
Department of Health and Mental Hygiene
Office of Operations and Pharmacy

Stephen H. Johnson
General Counsel
MedChi

Eileen Koski
Director, Informatics Research
Quest Diagnostics

Darren Lacey
Chief Information Security Officer
Johns Hopkins University/Medicine

Roger F. Leonard, M.D., F.A.C.P., F.A.C.C.
Vice President for Medical Affairs
Montgomery General Hospital

Peggy Leonard, R.N., NHA
Senior Director
Business Systems Operations
Genesis Healthcare

Thomas L. Lewis, M.D.
Chief Information Officer
Primary Care Coalition

Fred Magaziner, D.D.S.
Dental Compliance Officer
Department of Health and Mental Hygiene,
Board of Dental Examiners

Patti Maguire, R.N.
Branch Administrator
Personal Touch Home Care

Ellen Maltz
Practice Consultant
Montgomery County Medical Society

Susan Miller, M.D.
Medical Director
MedStar Health

Linda Minghella
Director, Information Technology
Civista Medical Center

Stanley Nachimson
Principal
Nachimson Advisors, LLC

DeWayne Oberlander, MBA, MPH
Executive Director
Columbia Medical Practice

Chris Panagiotopoulos
Technical Director, Security Officer
LifeBridge Health

Michael Penn, PMP
Manager, Health Information Technology
Erickson Retirement Communities

Traci Phillips
Director, Health Care Finance
Maryland Hospital Association

Carol Richardson
Chief Privacy Officer
Johns Hopkins Health System

Beth Sammis, Ph.D.
Vice President Corporate Communications
United Healthcare

Glenn Schneider, MPH
Executive Director
Maryland Healthcare for All

Liza Soloman, MHS, DrPH
Co-Chairman
AIDS Legislative Council

Bruce Taylor, M.D.
Psychiatrist
Shepherd Pratt Health System

Angelo Voxakis, PD
President, Chief Executive Officer
EPIC Pharmacies

Martin Wasserman, M.D., JD
Executive Director
MedChi

Daniel Wilt
Chief Information Officer
Erickson Retirement Communities

Grace Zaczek
Executive Director
Maryland Community
Health Resources Commission

Ronald A. Zoppo
IT Director, North Atlantic Division
Laboratory Corporation of America

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

Website: mhcc.maryland.gov
Telephone: (410) 764-3460   Fax: (410) 358-1236