MARYLAND
HEALTH CARE
COMMISSION

An Assessment of Privacy and Security Policies and Business Practices

Their Impact on Electronic Health Information Exchange

November 2007

Marilyn Moon, Ph.D.
Chair

Rex W. Cowdry, M.D.
Executive Director

4160 Patterson Avenue
Baltimore, Maryland 21215

Maryland Health Care Commission

The Maryland Health Care Commission (MHCC) is a public, regulatory commission established in 1999 by the Maryland General Assembly through the merger of the Health Care Access and Cost Commission with the Maryland Health Resources Planning Commission. The MHCC mission is to plan for health system needs, promote informed decision making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policymakers, purchasers, providers, and the public. The MHCC is administratively located within the Maryland Department of Health and Mental Hygiene, and is composed of 15 members appointed by the Governor, with advice and consent from the Senate, for a term of four years.

Commissioners

Marilyn Moon, Ph.D.
Chair

Gail R. Wilensky, Ph.D.
Vice Chair

Reverend Robert L. Conway

Garret A. Falcone, NHA

Tekedra McGee Jefferson, Esquire

Sharon K. Krumm, R.N., Ph.D.

Jeffrey D. Lucht, FSA, MAAA

Barbara Gill McLean, M.A.

Roscoe M. Moore, Jr.,
D.V.M., Ph.D., D.Sc.

Kurt B. Olsen, Esquire

Sylvia Ontaneda-Bernales, Esquire

Darren W. Petty

Andrew N. Pollak, M.D.

Sheri D. Sensabaugh

Nevins W. Todd, Jr., M.D.

Acknowledgements

This report would not have been possible without the assistance of Irene Battalen, Bernie Truffer, William Chan, and Madeline Sailes-Carlton of the Center for Health Information Technology. Special thanks go to Karen Rezabek and Nicole Stallings for editing the report. The Commission thanks all the Sector Group participants who gave their time to provide support to staff in pulling together the data and participated in the Sector Group discussions. The Commission appreciates the work of Avalere Health, LLC, and Strategies for Tomorrow, the consultants that provided support to this project.

Table of Contents

Executive Summary

1. General

The Maryland Health Care Commission (MHCC or Commission) is dedicated to promoting the quality and efficiency of health care in Maryland. Over the last 14 months, the Commission conducted an assessment of privacy and security policies and business practices related to electronic health information exchange from the perspective of eight health care Sector Groups. The assessment focused on business policies and practices in general, and security policies and practices in particular, that could hinder the development of effective electronic health information exchange either within hospital systems or statewide. A Sector Group was organized for each of the following health care sectors: consumer, hospital, medical laboratory and diagnostic imaging, long term care, payer, pharmacy, physician, and purchaser.

Electronic health information exchange promises to bring vital clinical information to the point-of-care, helping to improve the safety and quality of health care while decreasing overall health care costs. Nationwide, interest in sharing electronic patient information has been on the rise since the 2004 Presidential Executive Order that called for most Americans to have access to an interoperable electronic health record by 2014.[1]

In 2001, the Institute of Medicine concluded that health information technology (HIT) had enormous potential to improve the safety, quality, and efficiency of health care.[2] The Sector Groups participating in the MHCC privacy and security assessment believed that exchanging health information electronically offers many advantages over the current paper system. Comprehensive patient health information can be available at the time and place of care, be linked to clinical decision support systems, and provide information about quality, outcomes, and cost. Better information empowers both patients and providers, and promotes the choice of evidence-based care based on demonstrated value. Electronic health information exchange can also result in more relevant and less costly clinical and health services research, in addition to cost-effective surveillance for adverse drug effects, threats to homeland security, and emerging infectious diseases.

The eight Sector Groups participating in the assessment agreed that a statewide electronic health information exchange should be implemented. Participants were largely in agreement that data sharing should occur initially within hospital systems, and be utilized by the providers participating in that system. Many of the participants believed that health information exchange should develop both within hospital systems and statewide, and that they should do so simultaneously and not in isolation of each other.

[1] The White House, *Executive Order: Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator* (Washington, D.C.: Office of the Press Secretary, April 27, 2004).
[2] Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century*, (Washington, D.C.: National Academy Press, 2001).

Sector Group participants recommended that the State facilitate the development of a statewide electronic health information exchange. Absent State involvement, some feared that any electronic health information exchange will be fraught with uncertainty and confusion. The Sector Groups also believed that a statewide electronic health information exchange should be a public-private partnership. Participants felt very strongly that sound policies addressing access, authorization, authentication, privacy and security need to be developed. They also agreed that hospital system initiatives would likely vary in business model design, and that business models need to be flexible and evolve as electronic health information exchange gains momentum.

The Sector Groups identified public trust as fundamental to successful health information exchange – both the trust of those involved in health information exchange and the trust of the general public. Currently, patients receive treatment in a health care system that is heavily dependent on paper, information is stored individually by providers, and accessing that information is difficult for both providers and consumers. Limited consumer access and control of patient information compounds this problem; patients are often disengaged from participating in decisions regarding treatment. The Sector Groups acknowledged that the lack of consistent privacy and security policies and business practices will slow down any attempt to implement electronic data sharing technology.

The majority of participants believed that addressing privacy and security barriers to electronic health information is necessary for widespread adoption of electronic health information exchange. Transforming the way health care information is used and stored in Maryland requires more than simply acquiring technology and applying it to existing processes and practices. The MHCC privacy and security assessment identified key policy questions and barriers to implementing a statewide electronic health information exchange.

2. Limitations

This report documents the work of the eight Sector Groups that assisted the MHCC with the identification of barriers and risks related to the privacy and security of electronic health information exchange. The assessment examined how organizational business policies and practices, as well as State and federal laws regarding privacy and security, affect electronic health information exchange. The findings of this assessment, while broad in scope, represent the views of the Sector Group participants, and are not intended to provide an exhaustive list of every privacy and security exchange issue in Maryland. Many more barriers and risks pertaining to privacy and security could potentially be identified beyond those contained in this report.

3. Sector Groups

a. Consumer

The Consumer Sector Group believed that electronic health information exchange would have far reaching benefits for all Marylanders. They also agreed that significant privacy and security concerns need to be resolved before they would feel secure about sharing sensitive information electronically.

Patients want to be able to control the flow of information that is released, as well as decide who has access to their health information. Participants agreed that an opt-out policy, in which patient information is included in the exchange unless patients explicitly exclude it, is the best approach to ensure adequate patient participation and administrative efficiencies. The Consumer Sector Group believed that registering patients in the exchange, as well as authenticating them, should in most cases be the responsibility of the primary care provider. In addition, users of the system should be identified through multi-factor authentication. They also felt strongly that an exchange needs to have well-established audit trails and electronic consumer alerts when patient information is accessed.

b. Hospital

The Hospital Sector Group believed that a business case for electronic health information exchange exists within each hospital system. At the present time, most hospitals are focused on using their resources to connect internal disparate systems and evaluate opportunities for sharing electronic patient information with providers in their service areas. Hospitals are not comfortable allowing other hospitals to have access to their patient information. The Hospital Sector Group viewed data as proprietary and as the leading method for maintaining market share. Participants cited improvement in the quality and efficiency of patient care as the primary benefit of electronic health information, achieved primarily through enhanced access to patient data and test results. Participants believed that the costs of development are the leading barrier to health information exchange, followed closely by the lack of consistent business practices and privacy and security policies.

c. Long Term Care

The Long Term Care Sector Group viewed their fragmented use of technology as a key barrier to moving forward with electronic data sharing. The key reasons for the lack of health information technology adoption in this sector were related to high employee and patient turnover, as well as low reimbursement. Participants viewed the primary benefits of health information exchange as the ability to make more informed patient care decisions, the ability to access information more rapidly through results delivery, and the cost savings associated with increased efficiencies in the care delivery process. An overall lack of education and awareness of health information exchange, and a fear of falling too far behind in the use of technology were major concerns. Participants felt that the State needs to establish policies on privacy and security before patient information is electronically exchanged.

d. Medical Laboratory and Diagnostic Imaging

The Medical Laboratory and Diagnostic Imaging Sector Group currently uses technology to exchange patient information with providers. However, the Medical Laboratory and Diagnostic Imaging Sector Group noted that most physicians lack the infrastructure to support electronic health information exchange. Participants believed that expanding electronic health information exchange beyond lab and imaging results would increase the efficiency and quality of health care, and reduce operating costs. Medical laboratories maintain hundreds of costly provider connections to support different provider technologies. Diagnostic imaging centers reported administrative challenges in storing and forwarding images. Concerns were raised over the lack of national and local privacy and security policies, potential consumer resistance, disparities in the level of technology across sectors, and the impact of reduced revenues relating to duplicate testing that would be nearly eliminated as a result of information sharing. Participants that provide services nationally were also concerned about supporting different electronic health information exchanges in multiple states.

e. Payer

The Payer Sector Group reported skepticism about the overall value proposition in electronic health information exchange. Participants had mixed views on whether the benefits of electronic health information accrue primarily to payers, as compared to other Sector Groups. The Payer Sector Group noted that investing in systems to support electronic health information exchange would be difficult to justify given the length of time necessary to realize an appropriate return on investment. Participants were uncertain whether a statewide exchange is a wise decision at this time. They agreed that it is important to provide more information at the point of care, and they encouraged hospital systems to move forward to develop service area exchanges as the first step in building a statewide exchange. Participants were concerned about the lack of statewide privacy and security policies.

f. Pharmacy

The Pharmacy Sector Group reported that electronic health information exchange would create efficiencies and improve patient safety. Participants agreed that eliminating paper prescriptions will reduce the risks associated with handwritten prescriptions, and speed up the process of filling prescriptions. The pharmacy sector has a long history of using technology, and most participants reported the existence of sound policies and business practices to guard against inappropriate use and disclosure of electronic health information. Participants agreed that statewide privacy and security policies are needed, which should build upon the existing HIPAA regulations. There were concerns within the sector regarding physician reluctance to use technology, as evidenced by the slow adoption of electronic prescribing. Participants cited this as the leading barrier to electronic health information exchange.

g. Physician

The Physician Sector Group ranked improvements in efficiency and quality of care as the leading benefit of electronic health information exchange. Participants agreed that implementation of an exchange would reduce medical errors, increase operating efficiencies, advance pay for performance initiatives, and allow for more consistent use of evidence-based medicine. Reduced productivity during technology deployment was cited as a barrier to widespread adoption. Participants believed that increased use of health information technology will raise their liability exposure, and many felt that a business case for electronic health information exchange has not yet been made, and that incentives to adopt health information technology are misaligned. The Physician Sector Group was concerned that physicians will absorb the bulk of implementation costs when the benefits accrue primarily to other Sector Groups. Participants agreed that the State needs to consider financial incentives to expand technology adoption, and take the lead in developing a statewide exchange. In addition, the State needs to facilitate the development of privacy and security policies relating to health information exchange.

h. Purchaser

The Purchaser Sector Group agreed that purchasers would be a leading beneficiary of electronic health information exchange. Participants 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 a system of data sharing has been fully implemented. Most participants agreed that benefits resulting from improved health status will vary based upon industry. Participants believed that social and economic factors need to be considered when developing an exchange. Participants stated that any system of health information exchange must target the heavy users of health care services. Some concerns were expressed about the ability of purchasers to participate in funding electronic health information exchange. Participants felt that any funding arrangement should be based on employer size and industry. Concerns regarding the lack of privacy and security policies were viewed as the leading barriers to implementation, followed closely by the costs associated with purchasing or upgrading existing computer systems and hiring additional staff.

4. Recommendations

Electronic health information exchange has enormous potential to improve the safety, quality, and efficiency of health care delivery for consumers throughout Maryland. Implementing an exchange also has associated risks and barriers. MHCC’s assessment of business policies and practices in general, and security policies and practices in particular, is a first step toward addressing the barriers to electronic health information exchange.

The following recommendations were based on the work of the eight Sector Groups:

- Develop statewide policies to address access, authorization, authentication, and the privacy and security of electronic health information.

- Resolve issues relating to ownership and control of electronic health information.

- Encourage hospital systems to foster development of data sharing with service area providers.

- Move forward in developing a statewide electronic health information exchange.

- Develop consumer education initiatives relating to electronic health information exchange.

- Explore State funding opportunities in the form of grants and small business loans for provider acquisition of health information technology.

- Resolve concerns over increased provider liability with electronic health information.

- Develop a standard set of data that can be used for sharing information within a hospital system and in an exchange.

- Determine data uses for purposes other than treatment, payment, or health care operations.

- Consider the broad impact of personal health record adoption on electronic health information exchange.

- Develop legislation that includes incentives for health information technology adoption, and explore the impact of mandating its use by 2014.

Overview

The Maryland Health Care Commission (MHCC) conducted an assessment of privacy and security policies and business practices related to electronic health information exchange from the perspective of individual health care Sector Groups. The Sector Groups consisted of consumers, hospitals, medical laboratories and diagnostic imaging centers, long term care providers, payers, pharmacies, physicians, and purchasers. MHCC conducted field interviews and engaged two consultant organizations, Avalere Health, LLC and Strategies for Tomorrow, to assist in gathering additional data, conducting analysis, and drafting a preliminary report for each Sector Group. The work focused on business policies and practices in general, and security policies and practices in particular, that may hinder the development of effective local, regional, and national systems for electronic health information exchange.

Electronic health information exchange offers many advantages over the current system of sharing information. Comprehensive health information about the patient, using electronic health record (EHR)[3] systems, can be available at the time and place of care, linked to clinical decision support systems, and tied to information about quality, outcomes, and cost. An EHR is defined as a longitudinal electronic record of patient health information, and can be used to provide information that empowers both patients and providers, and promote evidence-based care. Technology in and of itself does little to create value; optimally used, however, it can provide the means to realize improvements in quality and patient safety. Electronic health information exchange has the potential to make clinical and health services research more relevant and cost-effective, and provide surveillance for adverse drug effects, threats to homeland security, or emerging infectious diseases. A RAND Health study reported that health information technology could save a minimum of $77 billion annually in efficiencies, and provide an annual savings of about $1 billion.[4]

MHCC's assessment of privacy and security policies and business practices revealed key barriers to electronic health information exchange in the State. The next step is to identify solutions and implementation plans that adequately address these barriers.

1. Assessment

The assessment began with an examination of how each Sector Group viewed electronic health information exchange, in terms of both its promise and potential pitfalls. Sector Groups identified the issues of greatest concern, as well as how governance, privacy and security policies, business practices, changes in State and federal laws, and new technologies might be used to address these concerns and build public trust. The Sector Groups also considered the barriers, risks, and challenges related to electronic health information exchange. The Sector Groups viewed the trust of both the multiple stakeholders in electronic health information

[3] The Healthcare Information and Management Systems Society defines an electronic health record (EHR) as a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. http://himss.org/ASP/topics_ehr.asp.

[4] Rand Health, *Health Information Technology, Can HIT Lower Costs and Improve Quality?* (Santa Monica, CA: Rand Corporation, 2005), 2.

exchange and of the general public as fundamental to successful electronic health information exchange.

Sector Groups were given latitude in choosing how to complete the following activities:

a. **An assessment of the degree of knowledge, as well as concerns and opinions, about the use of electronic health information exchange, including:**

   1) Concerns regarding the privacy and security of health records with the expanded use of electronic health information exchange, and perspectives on whether these concerns could be addressed sufficiently to obtain widespread support by patients.

   2) Opinions regarding the costs and benefits of the wider use of electronic health information exchange.

   3) Opinions regarding the adoption of personal health records (PHRs) based on their potential to promote quality improvement and error prevention.

   4) Prominent reservations about the wider use of electronic health information exchange, and the ways in which those reservations might be addressed.

b. **An assessment of the potential advantages and disadvantages of comprehensive electronic health records, and the development of specific suggestions that address each area of concern about privacy and security in a consistent way across all Sector Groups.**

   1) Methods for protecting particularly sensitive information, such as psychiatric records or HIV status, and whether special access restrictions should be implemented to protect this information.

   2) Methods for authenticating patient identity.

   3) Provisions for patient access to electronic health information.

c. **An assessment of privacy and security concerns related to the exchange of information between Sector Groups.**

   1) Determine issues related to development of a trust hierarchy for the exchange of health information with other health sectors.

   2) With respect to interoperability, whether a standard set of information should be identified when exchanged between Sector Groups in specific situations.

   3) To help assure appropriate health care and prevent errors, whether a standard set of information should be identified when exchanged within the same Sector Group.

Sector Groups were also asked to recommend potential solutions that address privacy and security concerns, and improve access, quality of care, and lower costs. These solutions were based on the health care needs and demographics of the populations represented by Sector Group participants, as well as their ability to use electronic health care information.

2. Sector Groups

Representation at each Sector Group meeting varied between ten to twenty individuals. Participants held key leadership positions within their respective organizations, and many had years of experience in direct patient care. Each Sector Group met an average of six times, using a combination of in-person and virtual meetings.

Sector Groups were tasked with providing their unique perspective relating to:

a. Benefits of electronic health information exchange, including those benefits from the use of electronic health records and PHRs.

b. Perspectives on privacy and security of personal health information, including how they may act as barriers.

c. Key issues such as governance and privacy and security policies that might facilitate multi-stakeholder trust and adoption of electronic health information exchange.

Strategies for Tomorrow facilitated the meetings of the physician, hospital, payers, and medical laboratory and diagnostic imaging Sector Groups. Avalere Health, LLC facilitated meetings of the consumer and long term care Sector Groups. MHCC facilitated meetings of the pharmacy and purchaser Sector Groups. Both consultant organizations assisted MHCC in an Inter-Sector symposium, which consisted of at least two representatives from each Sector Group. The Inter-Sector symposium was aimed at building on the work of the Sector Groups, and discussing potential solutions to maintain the privacy and security of electronic health information.

Background on Health Information Exchange

1. General

The delivery and management of health care has extended beyond the walls of a single provider. As a result, health information is located across multiple provider settings where paper and electronic patient information is stored in information silos. Today, information sharing is largely through facsimile or paper records. Providers often employ staff whose sole function is to request, collate, and file clinical data supplied by other health care providers, or to respond to similar requests from these providers. Health information technology (HIT) holds the promise of improving health care. While the initial investment and ongoing costs of HIT are borne by providers, the benefits are shared across Sector Groups, with most realized by payers through reductions in costs associated with fewer errors, reductions in duplicative and unnecessary care, greater formulary compliance, and improved disease management.[5] A concern shared by many Sector Groups is that the current reimbursement system does not incentivize or reward providers for quality improvement using HIT.[6]

Health information exchange (HIE) makes it possible for health information to move with the patient so that it is available wherever and whenever care is rendered. Electronic patient information can be particularly useful for patients with chronic conditions that are managed by multiple providers.[7] The Institute of Medicine's report, *To Err is Human: Building A Safer Health System,* released in November 1999, describes a comprehensive strategy by which health care providers can use technology to provide more effective care and reduce preventable medical errors.

HIE requires expensive, sophisticated technological interfaces, and standards must be developed to communicate health information across health sectors. This has broad implications beyond cost. Achieving interoperability requires expending a significant amount of time and effort to develop standards and business practices. Standards and business practices cannot be created and imposed without significantly affecting those providers that have already invested financial and human resources to implement HIE. Concerns regarding privacy and security, access, authentication, authorization, and appropriate use and disclosure are significant issues that need to be addressed if HIE is to succeed. Beyond the basic technology and policy issues, users of HIE must also protect themselves through careful legal assessment and specific, carefully crafted data use agreements relating to the exchange of health information.

While the ultimate goal is to share health information statewide, there are compelling reasons for starting the process by developing the infrastructure locally at the hospital system level. Health care services are usually provided within the community. Data sharing and data use agreements will be much easier to develop and control at the local level.

[5] Sheera Rosenfeld, et al., "Financial Incentives: Innovative Payment for Health Information Technology,*" Foundation for eHealth Initiative*, March 2004, 8, http://www.leapfroggroup.org/media/file/Leapfrog-Financial_Incentives.pdf.
[6] Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century*, (Washington, D.C.: National Academy Press, 2001).
[7] Gerard F. Anderson, "Medicare and Chronic Conditions," *New England Journal of Medicine*, 353(3), (July 21, 2005): 307.

Hospital systems can also become de facto demonstration projects for other hospital systems around the State.

The eHealth Initiative review of the experiences of states, regions, and communities indicates that the groups experiencing the greatest success implementing HIE share the following characteristics:[8]

a. They are governed by a diverse and broad set of community stakeholders;

b. They have developed and assured adherence to a common set of principles and standards for the technical and policy aspects of information sharing, addressing the needs of every stakeholder;

c. They have developed and implemented a technical infrastructure based on national standards to facilitate interoperability;

d. They have developed and maintained a model for sustainability that aligns the costs with the benefits related to HIE; and

e. They use metrics to measure performance from the perspective of patient care, public health, provider value, and economic value.

2. Federal Activity

In 2004, the President issued an Executive Order that provided leadership for the development and implementation of a nationwide HIT infrastructure intended to improve health care quality and efficiency.[9] This Executive Order created the Office of the National Coordinator for Health Information Technology (ONC). As a result of the ONC's efforts, a number of initiatives are underway that address HIT issues. Although ONC has been tasked with promoting HIT across the nation, it does not oversee federal agencies that actually fund or provide health care, which falls to other areas within the Department of Health and Human Services (HHS).[10] Federal agencies and their HIT initiatives include:

a. The Centers for Medicare & Medicaid Services (CMS)

CMS administers the Medicare and Medicaid programs, which provide health care to about one in every four Americans. As the nation's single largest payer, CMS promotes the use of HIT to support states in their efforts to achieve safe, effective, efficient, patient-centered, timely, and equitable care.

[8] "eHealth Initiative Foundation's Second Annual Survey of State, Regional and Community-Based Health Information Exchange Initiative and Organizations" (*eHealth Initiative*, August 2005). http://www.ehealthinitiative.org/pressrelease825A.mspx.

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

[10] U.S. Department of Health and Human Services, *HHS: What We Do*. (Washington, D.C.: HHS Press Office, May 2007). http://www.hhs.gov/about/whatwedo.html.

b. The Agency for Healthcare Research and Quality (AHRQ)

AHRQ supports the nation's 10-year strategy to bring health care into the 21st century by advancing the use of information technology research on health care systems, health care quality and cost issues, access to health care, and effectiveness of medical treatments.

c. The National Institutes of Health (NIH)

NIH supports over 38,000 research projects nationwide and uses HIT to provide, coordinate, and advance computational science in the pursuit of knowledge about the behavior of living systems, and the application of that knowledge to extend healthy life and reduce the burdens of illness and disability.

d. The Health Resources and Services Administration (HRSA)

HRSA provides access to essential health care services to those who are low-income, uninsured, or who live in rural areas or urban neighborhoods where health care is scarce. HRSA promotes HIT to improve access to health care services for people who are uninsured, isolated, or medically vulnerable.

e. The Indian Health Service (IHS)

The IHS provides health services to 1.6 million American Indians and Alaskan Natives who represent more than 550 federally-recognized tribes. The IHS captures clinical and public health data through a variety of systems that allow providers to manage all aspects of patient care electronically, which starts before the patient is seen and continues through follow-up care.

f. Department of Defense (DoD)

The DoD serves an integral role in the United States and around the world in the area of security, humanitarian aid, peacekeeping, and disaster relief. The DoD recently launched a global EHR system to serve more than nine million service members, retirees, and their families worldwide.

g. Veterans Health Administration (VHA)

The VHA is a division of the U.S. Department of Veterans Affairs, and provides care for over five million veterans of the United States Armed Services. The VHA uses HIT to empower individuals to take a more active role in managing their health and health care.

3. Health Information Exchange Initiatives

Hospital systems are organizing across the State to connect providers for the purpose of exchanging clinical information. These organizations are usually geographically-defined entities which develop and manage a set of contractual conventions and terms, arrange for the means of electronic exchange, and develop and maintain exchange standards. Many hospital systems are beginning to collaborate and develop a consensus among diverse stakeholders in their service network to formulate a vision, goals, and plans that foster improved health care and outcomes through timely and appropriate health information exchange.

4. HIPAA and the Medicare Electronic Prescribing Rule

a. HIPAA

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that protect the privacy of protected health information (PHI), ensure the security of electronic information,[11] and define a set of technical standards for the exchange of administrative transactions.[12] PHI refers to individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, paper, or oral), but excludes certain educational records and employment records.

1) Privacy Rule

The HIPAA Privacy Rule, which went into effect on April 14, 2003, provides the first national standards for protecting the privacy of health information. It defined three types of covered entities that are required to follow HIPAA Privacy provisions: health plans, health care clearinghouses, and health care providers that conduct health care transactions electronically. Covered entities are required to implement policies and procedures that protect the use and disclosure of PHI, and provide patients with the ability to access or amend their information.

The Privacy Rule protects certain information that covered entities use and disclose, and generally entitles individuals to access their health records. Covered entities can use and disclose PHI without patient authorization for treatment, payment, or health care operations. The Privacy Rule defines the uses and disclosures of PHI that do require patient authorization, and establishes requirements for covered entities with regard to their non-employee business associates (e.g., lawyers, accountants, billing companies, and other contractors) whose relationship with covered entities requires sharing of PHI. Covered entities are required to provide patients with a Notice of Privacy Practices, which defines how the entity uses and discloses patient information at certain steps along the care cycle and at select times thereafter. The Privacy Rule does not cover employers, certain insurers (e.g., auto, life, and workers' compensation), or those public agencies that deliver social security or welfare benefits, when functioning solely in these capacities. The Privacy Rule does not supersede more stringent State law. Conversely, if a State law is less stringent than HIPAA, then HIPAA applies.

2) Security Rule

The purpose of the HIPAA Security Rule is to establish national standards for the protection of electronic PHI. The Security Rule, which became effective April 21, 2005, defines security standards to ensure the confidentiality, integrity, and

[11] 45 CFR Part 164, Subparts A, B,C, and E.
[12] 45 CFR Part 162, Subparts I through R.

availability of all electronic PHI that covered entities create, receive, maintain, or transmit. The Security Rule defines administrative, physical, and technical safeguards, and identifies standards that include risk analysis and disaster recovery, access authorization and authentication, and data encryption and integrity.

The Security Rule has 36 implementation specifications, which are further divided into two types: required (14) and addressable (22). Required specifications are essential, and covered entities must implement these specifications. However, covered entities have three choices for handling addressable specifications. They can implement an addressable specification if reasonable and appropriate, implement an alternative security measure to accomplish the purposes of the standard, or implement nothing if the specification is not reasonable and appropriate, and the standard can still be met.

3) Transaction Rule

The purpose of the HIPAA Transaction Rule is to adopt standards for administrative and financial health care transactions that are conducted electronically. This rule applies to the following types of health care transactions:

- Health claims and equivalent encounter information;
- Enrollment and disenrollment in a health plan;
- Eligibility for a health plan;
- Health care payment and remittance advice;
- Health plan premium payments;
- Health claim status;
- Referral certification and authorization; and
- Coordination of benefits.

A proposed standard for claims attachments was published in September 2005; a final rule is expected to be released in late 2007 or early 2008. The deadline for compliance with the HIPAA Transaction Rule was October 16, 2003.

b. Medicare Electronic Prescribing Rule

The Centers for Medicare & Medicaid Services' (CMS) final rule on electronic prescribing (e-prescribing) discusses the potential of e-prescribing to improve patient care and safety by reducing adverse drug events (ADEs). The e-prescribing final rule defined e-prescribing as "… the transmission, using electronic media, of prescription or prescription-related information, between a prescriber, dispenser, pharmacy benefits managers (PBMs), or health plan, either directly or through an intermediary, including an e-prescribing network. E-prescribing includes, but is not limited to, two-way transmissions between the point of care and the dispenser."[13] While there are no restrictions on the electronic transmission of Schedule I prescriptions in Maryland, federal regulations mandate that pharmacies maintain written prescriptions for Schedule II, III and IV controlled substances for two years. The Medicare e-prescribing rule also defines e-prescribing foundation standards for new prescriptions, refills, prescription changes, and prescription cancellations, and pilot standards for formulary information and medication history.

5. Maryland Confidentiality of Medical Records Act

Providers are also subject to the Maryland Confidentiality of Medical Records Act (MCMRA), which was enacted in 1991. A number of similarities exist between the HIPAA Privacy Rule and the MCMRA requirements. Generally speaking, both HIPAA and MCMRA address information shared in verbal, written, and electronic format. Both share broad similarities in permitting disclosure of patient identifiable information for treatment, payment, and health care operations. Both allow for disclosure without consent in emergency circumstances. Both permit using professional judgment when disclosing information to others involved in patient care. However, Maryland law is more stringent in two respects:

- MCMRA establishes a special category for mental health records, which are subject to different disclosure rules (HIPAA has similar provisions for psychotherapy notes); and

- MCMRA prohibits all redisclosures, unless specifically authorized by the patient or otherwise permitted.[14]

[13] Federal Register. Medicare Program: E-Prescribing and the Prescription Drug Program, Final Rule, 42 CFR 423, Vol. 70, No. 214, November 7, 2005.

[14] Office of the Attorney General, Maryland Health Care Commission, Department of Health and Mental Hygiene, the State Advisory Council on Medical Privacy and Confidentiality, with assistance from the Maryland State Bar Association Health Law Section, HIPAA Subcommittee, *Maryland Confidentiality of Medical Records Act Compared with HIPAA.* Department of Health and Mental Hygiene, *Privacy Statute & Regulation*: March 2003. http://www.dhmh.state.md.us/sacmpc/pdf/compchart.pdf.

Consumer Sector

1. Synopsis

The Consumer Sector Workgroup (Consumer Sector or Workgroup) consisted of representatives from consumer advocacy coalitions, mental health and disease advocacy groups, academic medical centers serving vulnerable populations, legal aid organizations, and providers serving the underserved or uninsured populations.

The Workgroup was asked to recommend potential solutions to address privacy and security concerns in order to improve access and the quality of care, and lower costs. These solutions were often based on the health care needs and demographics of the populations represented by the Workgroup members, as well as the ability of their constituents to use electronic health care information.

Participants believed that an opt-out policy, in which patient information is included in an exchange unless patients explicitly exclude it, would be the best approach to ensure adequate patient participation and administrative efficiency. The Workgroup also expressed a strong preference that the policy and technology allow patients to opt-out of the exchange at varying levels, e.g., by provider/facility, diagnosis, or type of prescription drug. Under an opt-out policy, a patient could prevent some or all of the data from a particular provider, as well as data about a particular diagnosis, from entering the health information exchange (HIE). The Consumer Sector recommended that the HIE use system flags to indicate that some health information has been excluded by the patient.

2. Workgroup Composition

The Workgroup consisted of representatives from ten organizations, each representing a unique perspective on privacy. The diversity of consumer perspectives held by the participants fostered an in-depth discussion of the issues. Participants identified the benefits and barriers of HIE, discussed how these barriers affect the exchange of data, and proposed solutions that promote the benefits of HIE while protecting the privacy and security of patient information.

The workgroup included:

Darrin Brown
Associate Director of Advocacy
AARP of Maryland

Michelle Carras
Outreach & Education Coordinator
NAMI of Maryland

Leigh Cobb
Coalition for Healthy Maryland Children
Advocates for Children and Youth

Erin Grace
Senior Vice President
Primary Care Coalition

Mary Jean Herron
Chief Financial Officer
Healthcare for the Homeless

Royal Riddick
Program Coordinator
NAMI of Maryland

Gretchen Derewicz
State Mission Delivery Director
American Cancer Society

Tina Ekeman
Healthcare for All

Carla Flaim
MIS Coordinator
Healthcare for the Homeless

Chris Gibbons, M.D., MPH
Associate Director
Johns Hopkins Urban Health Institute

Glenn Schneider
Executive Director
Maryland Healthcare for All

Liza Solomon, MHS, DrPH
AIDS Legislative Council

Vicki King Taitano
Legal Aid Bureau

3. State of the Sector in Maryland

Consumer awareness, as it relates to their ability to have input into the use and disclosure of their health information, is increasing throughout the State. Consumers are becoming more involved in managing their own health information through web based applications and the use of personal health records (PHRs). Several national payers doing business in Maryland allow their members to use technology for tracking health information. A number of private organizations have also implemented similar products.

4. Sector Readiness for Health Information Exchange

Participants agreed that consumer involvement and acceptance of HIE will likely increase in the future for many reasons. Patients are taking a greater interest in their health care. They are becoming more empowered to participate in their health care through several initiatives, such as the establishment of PHRs by employers, insurers and Medicare. As HIE efforts accelerate locally and nationally, the Consumer Sector believed that patients and consumers will increase their understanding of its benefits.

The Workgroup suggested that the State should take the primary role in sponsoring outreach and education to consumers as well as providers. Patients and consumers will need to understand their rights, the benefits and risks of HIE, and the positives and negatives of choosing to opt-out of an HIE. A consumer rights statement will be necessary for operational and enforcement purposes, and for patients to understand what rights and protections are available to them. The Consumer Sector envisioned the State overseeing the implementation of a statewide HIE. This would include the development and maintenance of a record locator service, and development of an opt-out mechanism. The Workgroup also saw a role for the State in guiding the development of policies related to privacy and security, user authentication, access, and authorization related to electronic PHI.

a. Personal health records and patient websites

A PHR is an electronic compilation of health information that is controlled by the patient. PHR products vary in appearance as well as sophistication. PHRs give patients control over permission to view, create, collate, annotate, modify, disseminate, use, and delete their records. PHR technology continues to evolve with the promise of accepting data, e.g., patient history, radiology and laboratory results, directly into the application from multiple provider sources.

Consumers are managing bank accounts, investments, and purchases using the Internet. They will eventually expect this same level of control to be extended to their online health portfolio. PHRs have been featured prominently in recent news stories, and both private and public initiatives continue to emerge. Leading examples include:

- A group of large employers, including Intel, Wal-Mart, and British Petroleum, announced a plan to provide PHRs to their employees.
- America's Health Insurance Plans (AHIP), an industry association of over 1,300 insurers, will test information portability through an 18-month PHR pilot project.
- The Robert Wood Johnson Foundation has funded nine grants to create a common set of applications as a platform for future PHRs.
- The Centers for Medicare & Medicaid Services (CMS) is funding a study to assess the feasibility of using Medicare claims data to populate PHRs, determine how best to communicate data from existing CMS systems to PHR technologies, evaluate information included in existing PHRs to best support beneficiaries' care, and to learn how existing PHRs address security and privacy issues.

The Workgroup believed that broader access to information through technology could dramatically increase health literacy and empower consumers. Today, more than 70,000 health information websites exist,[15] and an estimated eight of ten Americans search the Internet to locate health information.[16] Patient websites are offered by many entities including payers, employers, providers, technology vendors, disease management companies, disease advocacy groups, and pharmaceutical companies.

b. Privacy and security issues

The Consumer Sector felt strongly that privacy and security of PHI is vital to patients and critical to the acceptance of technology by consumers. Participants expressed some concern that emerging HIE and other technology initiatives are not held to the same standards established by HIPAA for protecting PHI.

[15] R. J. W. Cline and K. M. Haynes, "Consumer Health Information Seeking on the Internet: The State of the Art," *Health Education Research*, Vol. 16, no. 6, 2001, 671. http://her.oxfordjournals.org/cgi/reprint/16/6/671.

[16] Susannah Fox. "Online Health Search 2006, Most Internet Users Start at a Search Engine When Looking for Health Information Online. Very Few Check the Source and Date of the Information they Find." (Washington, D.C.: Pew Internet & American Life Project, October 29, 2006), 1. http://www.pewinternet.org/PPF/r/190/report_display.asp.

Organizations that exchange patient information, PHRs, and patient websites are not subject to HIPAA.[17] The Consumer Sector felt that at a minimum, HIPAA privacy and security protections should apply to technology that stores or transmits patient information.

Concern was also expressed that emerging technology could disadvantage patients with insurance companies or employers. Participants feared that insurance companies might raise premiums or deny coverage, and employers might make hiring and termination decisions based on health information.[18] The Consumer Sector noted that these concerns might initially delay patient acceptance of products aimed at improving health care.

c. Governance

One of the most important roles for a statewide HIE is to act on behalf of Marylanders by providing leadership for HIE efforts to promote the ethical and equitable use of private and secure patient information for quality, cost, access, and public health reasons. The Workgroup believed that the governance structure must be a public/private partnership that has sufficient authority to proactively promote HIE in the State. The Consumer Sector recommended creation of an autonomous, multi-stakeholder governing body to oversee the development of the following:

1) A vision and strategic plan;

2) A business model that includes financial sustainability;

3) Broad stakeholder representation; and

4) Technology and privacy and security policies.

Participants felt that a statewide HIE should be funded initially by the State. They also believed that a statewide HIE should encourage collaboration and cooperation between hospital system initiatives by working to develop a standard approach to HIE using a common set of guidelines, and to the extent possible, one which is based on quantifiable metrics.

5. Current Privacy and Security Practices

As recipients and users of the health care system, patients often function as gatekeepers of their own PHI. They place a high degree of trust in their health care providers to deliver care based on that information, and to keep that information confidential. The Consumer Sector believed that patients with some knowledge of HIPAA do not consider the requirements sufficient enough to protect their PHI once it is communicated to providers and documented in their health records. The Workgroup indicated its preference for greater protection of PHI, and more input into

[17] Angela Choy, et al., “Exposed Online: Why the New Federal Health Privacy Regulation Doesn’t Offer Much Protection to Internet Users.” (Washington, D.C. Pew Internet & American Life Project, November 2001), 7. http://www.pewinternet.org/PPF/c/5/topics.asp.

[18] Susannah Fox, et al., “The Online Health Care Revolution: How the Web Helps Americans Take Better Care of Themselves,” (Washington, D.C.: Pew Internet & American Life Project, November 26, 2000), 12. http://www.pewinternet.org/PPF/r/26/report_display.asp.

payer and provider use of information regarding treatment, payment, or health care operations.[19]

The Consumer Sector's understanding of HIPAA was somewhat fragmented. Participants felt that consumer expectations of HIPAA were driven by provider business practices. Workgroup members that represented provider organizations were the most familiar with HIPAA because it affects their daily operations. Other Workgroup members were fairly knowledgeable about HIPAA, particularly those representing vulnerable populations with sensitive conditions, such as HIV/AIDS, mental health, and substance abuse. As a result, the Consumer Sector viewed issues related to information access, privacy, and security through several different lenses, as well as their own sometimes frustrating personal experiences.

6. Benefits, Barriers, and Risks of Health Information Exchange

a. Benefits

The Consumer Sector thought that HIE will eventually be valuable to patients and consumers. The Workgroup believed that any efforts to develop an HIE must take into account the needs of the underserved population. They agreed that the leading benefits of HIE are better care in every setting and improved care coordination. Participants also noted that HIE would improve patient safety and drug safety, and viewed portability of patient information as essential to improving patient care.

b. Barriers

The Workgroup identified trust as a key barrier to HIE. Participants believed that patients do not trust how their health information is used, and were concerned that data might be used to deny insurance benefits or negatively affect employment status. Patients are generally unaware of how and when PHI is exchanged, and for what purposes. The Workgroup believed that providers, particularly primary care and family practice physicians, should serve as gatekeepers for access to electronic PHI.

Another key barrier to HIE is the uneven accessibility of electronic resources among consumers. While the digital divide is shrinking for some populations, such as for senior citizens, it still exists for many patients, such as minorities, low-income, and some vulnerable populations. In addition, many patients may not have immediate access to technology when they need to make decisions about controlling the flow of their PHI. This is a particular issue in crisis situations, such as admission to the emergency room, or in cases of impairment, such as for those in long-term care or rehabilitation facilities.

The Workgroup noted that cultural competencies have not been widely addressed in planning for HIE and other technology products. Participants pointed out that almost all HIT initiatives lack foreign language capabilities. The Workgroup said that HIE planning needs to address cultural competencies so that the information presented can be understood by all users.

[19] 45 CFR 164.506(c).

7. Consumer Sector Proposed Solutions

a. MHCC should lead the development of statewide privacy and security policies.

b. Patients should participate in HIEs on an opt-out basis.

c. HIEs should be required to give control over the flow of information to patients.

Hospital Sector

1. Synopsis

The Hospital Sector Workgroup (Hospital Sector or Workgroup) represented academic and community-based hospitals, and the Maryland Hospital Association (MHA). Participants agreed that absent sound privacy and security policies, health sector adoption of HIE would likely be fragmented, and gradual at best.

The Workgroup believed that a satisfactory business model can be developed to support a Maryland HIE. At the present time, most hospitals are focused on using their limited resources to connect diverse software applications within their own systems, and evaluating opportunities to share electronic patient information with community providers in their service areas. Participants believed that hospitals prefer to participate in HIE on a voluntary basis, and would not support mandates to implement a statewide HIE.

Improvement in the quality and efficiency of patient care was identified as the primary benefit of HIE, which would primarily be achieved by enhanced access to patient data and test results. Important pieces of clinical data are not always available or easily accessible without some form of HIE in place. The Workgroup agreed that building upon HIPAA privacy and security provisions are essential to advancing HIE in Maryland.

Stakeholder participation in an HIE requires an investment in the technology needed to support an exchange. This can cost a significant amount of money, which can vary by provider type and existing technology. The Workgroup concluded that a sustainable business model must be established in the early stages of developing an HIE, with the preferred model being one where those that derive the greatest benefit from the exchange absorb the largest share of the cost.

HIE has the potential to increase the inappropriate use of data by competitors and secondary users. While participants understood and support the need to share PHI, they were very concerned about other entities accessing data and using it for purposes other than treatment, payment, or health care operations. The Workgroup believes that without well-established privacy and security policies, data can be easily aggregated and used for marketing purposes. The Hospital Sector noted the existence of significant competition between Maryland hospitals for patients, particularly in the large metropolitan areas. Any statewide HIE effort must be carefully crafted so as not to negatively impact hospitals' competitive position in the marketplace. Concern was expressed about the impact of HIE on their ability to retain patients within their service areas.

Additional HIE concerns included the inadequate and inconsistent use of data and exchange standards, the potential for increased liability, and the difficulty of reaching agreement on the level of stakeholder contributions, participation, and voting rights in an exchange. Despite these concerns, most participants felt that exchanging data within local communities and across the State utilizing standardized formats can be achieved. The Workgroup indicated that nearly all hospitals are currently exchanging clinical data in some form with other service area providers. The

Hospital Sector also believed that existing standards should be leveraged to support development of a statewide HIE.

The Workgroup noted that hospitals have developed fairly stringent privacy and security policies to safeguard PHI. The Hospital Sector agreed that current policies need to be strengthened to accommodate statewide HIE. Current practices include safeguards for point-to-point data exchange between hospitals and other service area organizations, and only occur based on contractual agreements. Participants agreed that HIE creates new opportunities for inappropriate PHI disclosures, which may not be anticipated by existing business agreements.

The Hospital Sector viewed technology as an enabler of HIE and hospitals already have made significant investments in information technology. Participants felt that hospitals are better positioned to implement systems to support HIE than most of the other health sectors. Concerns regarding additional funding and the lack of consistent policy and business practices were considered a significant barrier to adoption of HIE.

2. Workgroup Composition

The Hospital Sector represented hospitals ranging in size and location around the State. Participants represented more than 5,000 acute care hospital beds statewide, which comprise approximately fifty percent of Maryland's licensed acute care beds.[20] The Workgroup had a thorough understanding of HIPAA privacy and security provisions, and was familiar with Federal government HIE initiatives.

The Workgroup included:

Douglas Abel
Vice President & Chief Information Officer
Anne Arundel Medical Center

Cathy Casagrande
Director of Health Information Management
& Privacy Officer
Frederick Memorial Healthcare System

Kenneth Davis
Assistant Vice President & CIO
Kennedy-Krieger Institute

Alexander Eremia
Associate General Counsel
MedStar Health, Inc.

Darren Lacy
Chief Information Security Officer
Johns Hopkins University & School of Medicine

Nisha Madhavan
Vice President
Hospital Audits, Services, Special Projects Support
Southern Maryland Hospital Center

Steve Mandell
Sr. Director, Clinical Information Systems
Johns Hopkins Medical Institutions

Linda Minghella
Director, Information Technology
Civista Medical Center

[20] Office of Health Care Quality, Department of Health and Mental Hygiene, *Acute, General and Specialty Hospitals*, Department of Health and Mental Hygiene, May 2007. http://dhmh.state.md.us/ohcq/licensee_directory/hosp-excel.xls.

Jeff Huddleston
Sr. Director, Information Technology
University of Maryland Medical System

Satish Jha
Health Care Information Mgmt. Exec.
Informatics Group
Adventist Health Care

Traci Phillips
Director, Health Care Finance
Maryland Hospital Association

3. State of the Sector in Maryland

The level of technology in Maryland hospitals is proportionate to size. Academic hospitals have fairly robust systems in place, while the use of technology in community hospitals varies by geographic location. Participants from large hospitals reported a readiness to participate in a statewide HIE. Technology investment reported by smaller hospitals is typically less and more closely tied to their current financial status. Several participants currently use web-based portals for communicating select clinical information with service area providers. The Workgroup felt that hospitals are much further ahead than most of the other health sectors in their use of technology.

4. Sector Readiness for Health Information Exchange

The Workgroup noted that hospitals have a long history of exchanging administrative data electronically with payers. Today, all hospitals are engaged in some form of electronic administrative transactions, primarily claims, remittance, and eligibility transactions with payers.

Most participants reported exchanging limited electronic PHI with service area providers. However, hospital exchange activity functions more along the lines of a web-based portal. Exchange partners include:

- Laboratories and imaging centers;
- Physician offices; and
- Pharmacies.

Participants reported using more stringent controls and safeguards for the access or release of sensitive information that is related to:

- Psychiatric treatment;
- Substance abuse;
- HIV status;
- Hospital employee records; and
- Famous persons.

5. Current Privacy and Security Practices

a. HIPAA compliance

Hospitals have spent hundreds of thousands of dollars complying with HIPAA privacy, security, and transaction & code set regulations. The Workgroup stated that most of the expense and effort devoted to HIPAA compliance was related to training staff on the appropriate use and disclosure of PHI, as well as retrofitting legacy information systems to accommodate new transaction formats. Participants have used HIPAA implementation as an opportunity to strengthen existing privacy and security policies.

The Hospital Sector agreed that most patients have a limited understanding of HIPAA regulations, and usually encounter them during registration when they receive and acknowledge receipt of the HIPAA Notice of Privacy Practices. Participants noted that patients are typically unaware of how providers use or disclose their PHI, and view the provider as the guardian of their most sensitive information and assume it is well protected.

b. Current authentication procedures, e.g., passwords, strength of passwords, changing of passwords, use of passwords and tokens

The Hospital Sector unanimously reported using role-based access, where users are given unique user IDs and passwords corresponding to specific functions and access to data within the hospital information system. Participants noted that passwords must be a certain combination of letters and numbers (strength), must be a certain length (usually 6-8 characters), and have expiration periods that require changing on a regular basis.

Today's widespread use of single-factor authentication is in the midst of change. Single-factor authentication methods, such as the basic username/password combination, are generally not considered strong enough. A number of participants reported using multi-factor authentication to gain system access. This approach to authentication provides a significant increase in security; the user name and password must be used in conjunction with tokens, smart-cards or even biometrics.

At a minimum, the use of multi-factor authentication improves the security and accountability of access to and modification of data as long as passwords are not shared. The Workgroup stated that hospitals have processes in place to routinely log and audit user access to specific systems and modifications to data, including additions, changes, and deletions.

Participants expressed concern regarding users who fail to log off a system prior to leaving a workstation. Many have implemented timed automatic logoff of users to address that issue. In some critical areas of hospitals, such as intensive care units, emergency rooms, and operating rooms, the automatic timeout feature is disabled, and those users typically share the same level of information access.

c. Methods for tracking access to medical records

The Hospital Sector reported using audit trails to track data access. The use of audit trails requires resources available to monitor and review audit logs on a regular basis. Many hospital information systems generate logs and reports that track additions, changes, and deletions to data. Thresholds can be set to track access by individuals, by time, or by terminals or locations. Participants noted that audit logs tend to be extremely large, and require careful review and a significant time commitment to identify outliers to established usage criteria.

The Hospital Sector restricts access to sensitive information, and limits access to small groups of users. Sensitive data, such as information about famous persons, hospital employees, psychiatric treatment, substance abuse, HIV status, and abortion, are segregated within hospital information systems and access to this information is controlled by user passwords and IDs. Policies are also in place which permit these records to be unlocked and accessed when necessary by specialized hospital departments, such as emergency departments.

d. Provisions for patient access to information

The Hospital Sector does not allow patients to electronically access their PHI. Patient requests for information are provided in paper form. Participants noted that release of patient information is subject to compliance with internal policies that are built upon the HIPAA Privacy Rule.[21]

e. Methods for authenticating the patient

The Workgroup reported consensus in the way patients are authenticated. Participants said that patient identity is authenticated during admission, primarily using picture IDs, such as driver’s licenses, whenever possible. When the admission process is completed, the patient receives a unique patient identification number, randomly assigned by the registration system, and a patient identification bracelet. These bracelets usually contain a barcode that identifies the patient, is affixed to the patient’s wrist, and is worn throughout the hospital stay.

f. Information audits

The Workgroup stated that most hospital financial audits include a hospital information system compliance review that evaluates internal security procedures, risk assessments, and business continuity plans. These audits typically confirm the existence of security policies, employee training programs, internal audit procedures and findings, as well as the management and reporting of security and business continuity activities. Participants said that financial audits tend to be helpful, but they did not believe that they assess privacy and security to the degree necessary for participation in a statewide HIE.

As covered entities under HIPAA, hospitals are required to designate a Security Officer.[22] Participants reported some variation in the role of the security officer, but agreed that they are typically a senior level person who is responsible for performing an organizational risk assessment, making security recommendations as part of an overall security plan, and executing audits that enforce the parameters of hospital security plans. Audits usually consist of user access and data integrity reviews. The Workgroup noted that most hospitals have over 100 policies to comply with HIPAA privacy and security requirements. In many cases, hospitals have implemented additional policies that go beyond HIPAA to help ensure the privacy and security of patient information.

[21] 45 CFR 164.510(b).
[22] 45 CFR 164.308(a)(2).

g. Administrative or physical security safeguards

The Hospital Sector reported significant investment in their information technology systems and supporting infrastructure. Multi-million dollar technology investments in data centers, networks, hardware, and end user workstations are often at the center of these infrastructures. Data centers are highly secure, climate controlled environments that are typically isolated from administrative work areas. These centers usually have additional physical access controls, may require escorts for entry, and may include video surveillance.

Data centers house data processing equipment and generally function as the communication focal point for the hospital. Disaster recovery and business continuity plans represent the primary administrative safeguards to protect the security of these environments. The Workgroup reported that business continuity plans are quite comprehensive, and address data backup and disaster recovery activities. Business continuity plans are tested on a regular basis, and the results of these tests are usually reviewed by internal and external auditors.

6. Benefits, Barriers, and Risks of Health Information Exchange

a. Benefits

The Workgroup believed that HIE can provide substantial benefits. These benefits include enhanced access to patient data, quality improvement, and increased efficiency. Participants agreed with the prevailing literature that a fully implemented HIE can save lives, reduce medical errors, and achieve cost reductions. In addition, some participants felt that HIE will enhance a hospital’s ability to measure patient outcomes more precisely, while several mentioned that efficiencies gained through electronic PHI will help strengthen the business case for provider adoption.

b. Barriers

The Hospital Sector identified funding as a leading barrier to implementing and sustaining an HIE. Hospital Sector participants estimated these costs to be around $20 million dollars for the first five years. While everyone agreed that an HIE would produce value to the system, participants expressed concern about adequately resolving the funding dilemma.

The Workgroup believed that a viable statewide HIE should start with a strong public-private partnership and broad Sector Group representation. The Hospital Sector had mixed views about the governance structure and how to appropriately give weight to the voting rights of individuals. Some participants believed that everyone should have equal weight in voting, while others thought that size should be the deciding factor. They were unanimous in their opinion that State participation is essential in any governance structure.

The Hospital Sector was concerned about how diverse consumer interests can be adequately represented in the governance structure. Participants felt that some consumer interests could be easily overlooked. Identifying a method to ensure adequate consumer representation in the governance structure remains a challenge that needs to be resolved.

The Workgroup agreed that data usage agreements should be developed by the governance structure, and should define:

- The appropriate use of data;
- Access controls and administration;
- Limits on secondary transmission of data;
- Limits on data aggregation;
- Restrictions for de-identified data;
- Notification procedures for incidental and malicious disclosures;
- Data ownership;
- Data integrity validation processes; and
- Auditing.

The Hospital Sector identified key policy barriers related to privacy, security, access, authorization, and authentication. Participants expressed disappointment over the lack of national HIE policy. They agreed that HIPAA is more applicable to paper records than to electronic health information, but viewed HIPAA as a foundation upon which to build more stringent policy protections. The Workgroup agreed that the State will be instrumental in developing the policy required to support a statewide HIE. Significant concerns were expressed regarding the secondary use of PHI. Participants had mixed views on whether data sharing and data usage agreements could provide adequate protection for the secondary use of data.

The Hospital Sector is concerned about its ability to retain community physicians in a statewide HIE. Today, hospitals that provide physicians with electronic access to patient information have a competitive advantage over other hospitals. HIE is expected to equalize this benefit across all hospitals, removing any incentives for physicians to remain affiliated with one particular hospital. Participants also acknowledged that a lack of consistent business practices is a significant barrier that needs to be resolved before an HIE can be implemented.

The Workgroup recognized the need to obtain stakeholder trust in HIE. Participants were guardedly optimistic that trust hierarchies can be established that will address issues related to competition, data security, and the ability of an HIE to safeguard information appropriately. Participants viewed the role of the State as critical to resolving trust issues.

7. Hospital Sector Proposed Solutions

a. Develop a standard data set that can be exchanged among service area providers.

b. Require all hospitals to establish connections with service area providers.

c. Develop privacy and security policies that can adequately support HIE.

d. Identify funding opportunities and financial incentives for providers to adopt technology.

e. Require hospitals to only use software products that are certified by the Certification Commission for Health Care Information Technology (CCHIT).[23]

[23] Three leading HIT industry associations (the American Health Information Management Association, the Healthcare Information and Management Systems Society and The National Alliance for Health Information Technology) joined forces in July 2004 to launch CCHIT as a voluntary, private-sector organization to certify HIT products. In September 2005, HHS awarded CCHIT a three-year contract to develop and evaluate certification criteria and create an inspection process for HIT.

Long Term Care Sector

1. Synopsis

The Long Term Care Workgroup (LTC Sector or Workgroup) consisted of representatives from skilled nursing facilities (SNF), home health agencies, community-based service providers, assisted living facilities, and hospices. The long term care patient population generally requires a broad range of care needs, resulting in a mix of providers caring for this segment of the population.

The Workgroup noted that the adoption of HIT in this sector is typically very low, primarily because profit margins tend to be small. Participants stated that finding products which meet their diverse needs is challenging. In addition, high staff turnover and uncertainty regarding the benefits of HIT have also adversely effected technology adoption. A majority of the Workgroup indicated that they intend to implement an electronic charting[24] system in the next six to 12 months.

Participants agreed that HIE would benefit long term care providers by giving them the ability to manage patient information and use it to make better informed care decisions. Participants noted that HIE would provide more timely access to information through results delivery, but were uncertain how to take advantage of any efficiencies that might be gained through improvements in care delivery.

The LTC Sector recommended the development of a set of minimum functions that all HIEs should be required to implement including: policies for privacy and security, information audit capabilities, flags to indicate missing or withheld information, and an established mechanism to correct/amend inaccurate information. The Workgroup stated that a minimum data set for sharing electronic information needs to be identified by a broad range of stakeholders.

The Workgroup recommended that participation in HIE should be voluntary for providers, and strongly preferred an opt-out policy for consumer participation. Issues that should be addressed by the State were identified, such as the utility and potential revision of the state's current single-disclosure law, and the potential for electronic information to become a "vehicle" to increase provider medical liability.

The Workgroup suggested that the State's role in an HIE should be to provide information on best practices, facilitate broad stakeholder dialogue, and assist small facilities in negotiating technology costs with vendors. In addition, the LTC Sector felt that the State should establish privacy and security policies for HIE, building on those mandated by HIPAA. The Workgroup endorsed a public-private partnership to develop a statewide HIE.

2. Workgroup Composition

The LTC Sector consisted of 11 members from long term care facilities, including representatives from nursing homes, community care retirement centers, home health agencies, skilled nursing facilities, and assisted living facilities.

[24] Electronic charting was described by the Workgroup as a basic, early edition of the much more extensive EHR. An electronic chart would include electronic versions of basic chart characteristics.

The Workgroup included:

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

Cherri Fleagle
Director of Resident Care
Summerville at Westminster

Steve Harner
Vice President, IS and Facilities
MedStar Health VNA

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

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

Randy Martin
Chief Financial Officer
Vindobona Nursing Home

Jennifer S. Miller
Vice President of External Affairs
Mid-Atlantic LifeSpan

Susan Miller, M.D.
Medical Director
MedStar Health VNA

Donna Taylor
Executive Director
William Hill Manor

Keith White
Administrator
Vindobona Nursing Home

Daniel Wilt
Vice President, Information Technology
Erickson Retirement Communities

3. State of the Sector in Maryland

Long term care is rather unique in that it involves multiple providers and services. Providers consist of home-based services, large integrated delivery systems, continuing care retirement communities, and independently-operated facilities. Participants noted that this population tends to have a high percentage of individuals with cognitive as well as physical challenges, many of whom must rely on surrogates for routine decision-making. Care needs for this population often range from minimal assistance with daily functions, to extensive levels of clinical care, such as dialysis treatments or assistance with daily living activities (e.g., bathing, feeding, and toileting).

The Workgroup reported that fragmentation in care delivery for the sector creates unique challenges for implementation of HIT. Small profit margins in the LTC Sector make HIT funding particularly challenging. The high cost of HIT implementation, maintenance, and ongoing training creates disproportionate burdens for long term care providers. The Workgroup felt that misaligned incentives create additional challenges, as those investing in technology may not consistently reap the benefits resulting from quality improvement, which often accrue to payers. Participants believed that almost all health sectors will need to take part in HIE in order to achieve its maximum benefit.

The LTC Sector agreed that HIE would benefit the sector through better care coordination when patients transition across care delivery systems, along with improved quality of care and more efficient care delivery. Participants felt that family and patient surrogate information needs could be more adequately addressed through HIE. The LTC Sector viewed HIE as a powerful way to meet the increasing demand for timely information in health care.

4. Sector Readiness for Health Information Exchange

The Workgroup felt that long term care has not adopted technology at the same level as other health sectors. The LTC Sector reported varying degrees of technology planning and implementation. The majority of participants reported that their organizations do not currently have technology in place to support electronic clinical information. A majority of participants reported the use of computers for billing and other basic administrative functions, such as registration and scheduling. Several participants said their use of technology is limited to completing the CMS minimum data set (MDS).[25]

5. Current Privacy and Security Practices

The Workgroup reported that their organizations are in compliance with HIPAA privacy and security regulations, but noted that interpretation and adherence varied across the sector. Most participants felt that HIPAA did not address the unique characteristics of the long term care. The frequent transition of long term care patients across delivery systems, ranging from acute care to rehabilitation to independent living, often creates challenges to appropriately manage privacy and security policies.

a. Authentication procedures

Participants stated that role-based access is currently the common practice in determining and authorizing access to paper-based information. Access to electronic information varies, depending on the size of the organization. Smaller organizations use single-factor authentication, issuing user names with weak password protections, while larger organizations have implemented strong password protections requiring a combination of alpha, numeric, upper and lower case, and special characters to gain access to systems. The LTC Sector emphasized the ongoing challenge of aligning workforce titles and roles to achieve consistent and secure role-based access.[26] A number of participants stressed that titles often have little correlation to the level of patient interaction or information access. They noted that employee access to patient information will vary in emergency situations. Where other health sectors might have clear role-based systems, this is not practical in most long term care settings. The Workgroup could not agree on a standard set of access procedures for long term care.

[25] The Minimum Data Set (MDS) is part of the U.S. federally mandated process for clinical assessment of all residents in Medicare or Medicaid certified nursing homes. This process provides a comprehensive assessment of each resident's functional capabilities. MDS information is transmitted electronically by nursing homes to the MDS database in their respective states on a quarterly basis. MDS information from the state databases is captured into the national MDS database at the Centers for Medicare & Medicaid Services (CMS).

[26] Role-based access is a policy and practice that grants data access rights based on a user’s role within an organization and specifically supports the “minimum necessary” standard of HIPAA. Role-based access can be difficult to implement. As the assignment of roles may vary across facilities, it must be applied consistently across all levels of the organization, and it requires that there are security measures in place, e.g., security IDs and passwords, to ensure appropriate access.

b. Method for tracking medical record access

The LTC Sector noted that most long term care electronic administrative systems lack the ability to produce user access audit logs. They indicated that some high-end systems offer some limited audit features, but most long term care facilities lack the technical resources necessary to conduct employee audits.

c. Provisions for member access to information

The Workgroup noted that the LTC Sector does not provide patients and consumers direct access to electronic PHI. Participants agreed that the technology to support web-based access to health information is not likely to be available in the foreseeable future. Well-established procedures exist in LTC for patients and consumers to access paper health records.

d. Member consent

The LTC Sector reported difficulty determining who can act on behalf of a patient. Oftentimes family members will want to have access to PHI or make treatment decisions on behalf of the patient when they do not have documented authority. Participants said that determining whether a patient is competent to provide consent for treatment, or determining who can sign on a patient's behalf, is an arduous process.

e. Administrative and physical security safeguards

The LTC Sector reported having sound administrative and physical safeguards in place for PHI. Most participants store information on paper and maintain it in areas that are supervised at all times. The Workgroup noted that terminals used to access electronic PHI are placed in areas supervised by staff, require appropriate logon by users, and time out after long periods of inactivity.

6. Benefits, Barriers, and Risks of Health Information Exchange

a. Benefits

The LTC Sector believed that HIE could provide value to patients and long term care facilities once it has been fully implemented. Participants noted that long term care adoption of technology will trail other health care sectors, due to both the cost and lack of a business case for adoption. The LTC Sector stressed that the value proposition has primarily focused on quality improvement and reduction of errors, and felt that this approach made it difficult to justify implementation costs. Participants agreed that HIE would provide them with the ability to efficiently manage large amounts of information and make more informed patient care decisions. They also felt that HIE could provide better access to more thorough medication lists, timely test results, and discharge summaries.

b. Barriers

The Workgroup reported that managing access to patient information, while maintaining the privacy and security of the information, is a significant barrier to implementing HIE. They cited the difficulty of protecting PHI in a way that will not interfere with existing work processes. Issues related to access, authorization, authentication, and patient consent need to be resolved before long term care providers could participate in HIE. They were particularly concerned about resolving patient consent issues, given the nature of the long term care patient population and their mental capacity. The Workgroup noted that the high employee turnover rate, estimated at 50 percent or greater,[27] and the challenge of maintaining access rights in a secure and timely manner as individuals are constantly added and deleted, was viewed as a barrier to implementing HIE.

7. Long Term Care Sector Proposed Solutions

a. Develop statewide privacy and security policies.

b. Resolve consent issues.

c. Develop incentives for funding technology specific to long term care.

d. Provide assistance to long term care to develop the business case for adoption of HIE.

[27] Edward A. Miller and Vincent Mor, *Out of the Shadows: Envisioning a Brighter Future for Long-Term Care in America,* (Brown University Center for Gerontology and Health Care Research, November 2006), 7. http://www.chcr.brown.edu/pdfs/brown university ltc report final. PDF.

Medical Laboratory and Diagnostic Imaging Sector

1. Synopsis

The Medical Laboratory and Diagnostic Imaging Workgroup (Lab and Imaging Sector or Workgroup) represented organizations that are fairly advanced in their use of HIT. This health sector has been exchanging electronic PHI for more than a decade. The Workgroup viewed this sector as somewhat ahead of other health sectors in addressing privacy and security policies. Participants agreed that more work is needed to establish exchange policies for participation in a statewide HIE.

The Lab and Imaging Sector expressed concern regarding the limited ability to communicate electronically with other health sectors. Participants noted that state laws require that test results be delivered only to ordering providers. There is also confusion with regard to the amount of information that should be released to Managed Care Organizations. Overall, the Workgroup felt that the most significant barrier to implementing HIE was related to cost. Other barriers identified by participants included the lack of national and local privacy and security policies, disparities in the level of technology adoption across health sectors, and the potential for the Lab and Imaging Sector to lose revenue as duplicate testing declines.

2. Workgroup Composition

The Lab and Imaging Sector included representatives from two national laboratories, one regional health care organization, and one regional radiology group. Participants had an information technology background and a clear understanding of the critical HIE policy questions.

Organizations in this sector varied widely in their size and structure, ranging from large, national, multi-state organizations to individual in-hospital laboratories and imaging centers. Participants represented organizations that provide services to over 200,000 patients annually in Maryland.

The Workgroup included:

Robert Stroud, M.D.
President
Advanced Radiology

Gail Glover
Director, Security Policy Administration & HIPAA
Quest Diagnostic

Robert Hennessy
Director, Systems Solutions
Laboratory Corporation of America

Eileen Koski
Informatics Division
Quest Diagnostics

Chris Panagiotopoulos
Technical Director & Security Officer
LifeBridge Health

3. State of the Sector in Maryland

The Workgroup reported that the majority of lab and radiology requests in the State are handled by national organizations. Participants noted that an increasing number of independent reference labs and imaging centers are connected to their referring community of physicians through web-based portals. The Lab and Imaging Sector participants viewed themselves as highly regulated, and subject to a number of State and federal requirements for licensing and certification that include:

- Clinical Laboratory Improvements Amendments (CLIA);[28]
- College of American Pathologists (CAP) National Laboratory Certification Program (NLCP); [29] and
- National Committee for Clinical Lab Standards (NCCLS).[30]

Both lab and Imaging centers are required to comply with HIPAA standards. Labs must comply with CLIA standards, while imaging centers are also required to comply with specific standards established by:

- Food and Drug Administration (FDA);
- Nuclear Regulatory Commission (NRC); and
- Maryland Department of Environment (MDE).

4. Sector Readiness for Health Information Exchange

The Workgroup reported that labs are fairly advanced in their adoption of HIE, as the industry has been using Laboratory Information Systems (LIS) for nearly 10 years. In contrast, technology adoption by imaging centers is not nearly as advanced. However, participants noted that imaging centers have been extremely effective using technology to improve operating efficiencies and expand services to providers.

The Lab and Imaging Sector reported that nearly all national imaging centers send a significant percent of their digitized images to overseas companies for interpretation by Maryland licensed and Maryland hospital-credentialed radiologists. The advantages of using this type of off-shore program are:

- Images are read by off-shore radiologists who interpret and transmit images during non-office hours; and
- Costs for off-shore radiologists are significantly less.

[28] Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services, *Clinical Laboratory Improvement Amendments*, (Washington, D.C.: U.S. Department of Health and Human Services, July 27, 2007). http://www.cms.hhs.gov/clia.

[29] "Accreditation and Laboratory Improvement" (College of American Pathologists, August 28, 2007). http://www.cap.org/apps/cap.portal?_nfpb=true&_pageLabel=accreditation.

[30] "About CLSI" (Clinical Laboratory Standards Institute, August 28, 2007). http://www.nccls.org/AM/Template.cfm?Section=About_CLSI.

a. Status of exchange with other sectors

Patient results are shared electronically with the following provider types:

- Hospitals;
- Physicians' offices;
- Payers;
- Public health departments; and
- Other labs and imaging centers.

The Workgroup noted that while most labs and imaging centers have technology in place to support electronic results reporting, providers lack the necessary technology to support bidirectional exchange of electronic health information. Participants noted that most providers request to have test results sent to them via facsimile, and several expressed some concern over the number of providers that continue to request paper. The Lab and Imaging Sector does not share information electronically with consumers, but hard copies of information are provided to patients upon receipt of appropriate authorization.

b. Current infrastructure

The Workgroup reported that most national labs have national networks in place, and many offer providers access to web-based portals for results retrieval. Imaging centers usually use web-based applications to transmit images, and providers can choose to participate in services that allow online viewing. Participants stated that labs experience an array of challenges when establishing and maintaining direct electronic connections with providers, while imaging centers reported little difficulty.

c. Plans for future adoption

Participants said they are already positioned to support the expanded use of HIT. They were enthusiastic about hospital system efforts to connect service area providers, as well as the development of a statewide HIE. The Workgroup encouraged the State to move forward in advancing HIE across all health care sectors.

5. Current Privacy and Security Practices

a. Current authentication procedures

The Workgroup believed that two-factor authentication should be the required minimum standard for authentication. Some participants have experimented with more robust authentication techniques, where access is based on something you know, something you have, and something you are, such as fingerprints or retinal scans.

b. Data access

The Lab and Imaging Sector reported that user access to electronic PHI is role-based. Participants said that employees are only allowed access to the information needed for their role within the organization. The Workgroup expressed some concern about the administrative challenges of sustaining organization-wide access controls. Some participants noted that national organizations find it difficult to administer role-based access on a timely basis. New employees, terminated employees, and employees whose access must be modified due to role or job changes within an organization create enormous work for system administrators. Participants also noted that system administrators routinely perform random audits to identify patterns of misuse. These reviews tend to be time consuming and labor intensive.

The Workgroup noted that consumers usually obtain test results from the ordering physician, but consumer requests for information are occasionally received directly. Requestors are required to complete a release of information form. The Lab and Imaging Sector does not have systems in place for consumers to electronically access information. They reported using stringent guidelines to release information for uses other than treatment, payment, or health care operations. The Workgroup's business practices for releasing PHI varied among participants, with some organizations not releasing information at all, and others releasing information after evaluation of requests by a formal Informatics Committee.

The Labs and Imaging Sector is unique in that ordering providers are their primary customers -- not patients. The unique relationship with providers exists because consumers do not initiate requests for ancillary services. Participants said that tests are only performed upon receipt of physician orders. Business practices varied in the way patient consent is handled, but everyone reported obtaining consent before services are provided.

c. Security architecture

The Lab and Imaging Sector participants noted that the HIPAA Security Rule is used as the foundation for developing security policies, but were unanimous in their belief that the Security Rule is insufficient to address HIE. Many labs comply with the certification requirements of the National Laboratory Certification Program (NLCP).[31] These guidelines establish scientific and technical standards that are used to certify laboratories that test specimens collected by Federal agencies. NLCP certification includes standards to ensure privacy and security of individuals.

[31] "National Laboratory Certification Program" (U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Division of Workplace Programs, August 28, 2007). http://www.workplace.samhsa.gov/DrugTesting/Dtesting.aspx.

d. Information protections

The Workgroup viewed their organizations as having strong policies that protect the privacy and confidentiality of PHI. Participants reported that sensitive data are stored in databases that segregate sensitive from non-sensitive data. Hardware and software used by this sector is designed to guard against external intrusion and control unauthorized access to data.

6. Benefits, Barriers, and Risks of Health Information Exchange

a. Benefits

The Workgroup believed that HIE will bring vital clinical information to the point of care. The Workgroup also expected that HIE would help improve the safety and quality of health care while decreasing overall health care costs.

A key benefit identified included the improvement in operational efficiency that electronic results delivery can provide to most providers. The ability to reliably access results at the point of care streamlines the workflow. Results are available when patients arrive for appointments; they do not have to wait for paper records to be faxed, or reschedule appointments because results are not yet available.

The Workgroup also believed that HIE reduces costs through streamlined workflows, reallocation of staff, and elimination of duplicate testing. It was also noted that duplicate testing often occurs because providers either do not have access to test results information, or believe the results are obsolete. Although reluctant to estimate the financial impacts, participants agreed that the effect of HIE on revenue could be sizable. There were mixed views on whether HIE can reduce treatment errors.

b. Barriers

Participants identified cost and a lack of privacy and security policies as the most significant barriers to implementing a statewide HIE. Participants believed that HIE implementation requires significant upfront investment, and questioned their sector’s ability to fund investment costs.

The Lab and Imaging Sector expressed concerns about consumer acceptance, a lack of technology readiness among health care sectors, and the potential for some providers to lose revenue as a result of information sharing. Additional concern was also expressed about the secondary use of data, and participants readily agreed that secondary use of PHI has not been fully addressed in any of the literature, or by existing HIEs.

Participants were concerned about how an HIE can establish trust and validate trust relationships. They were unsure how effectively trust agreements can safeguard information in an exchange. Additionally, it was noted that any perceived lack of trust will significantly impact provider participation and consumer willingness to have their data included in an exchange. Some participants were concerned about liability if patient information available through an HIE is not acted upon.

7. Lab and Imaging Sector Proposed Solutions

a. Address potential revenue implications that a statewide HIE will have on the Lab and Imaging Sector.

b. Develop privacy and security policies prior to implementing a statewide HIE.

c. Identify standard data sets for electronically exchanging information between providers.

d. Require hospitals to electronically connect with service area providers.

Payer Sector

1. Synopsis

The Payer Sector Workgroup (Payer Sector or Workgroup) included representatives from private and government payers, electronic health networks, and self-insured employers. The Workgroup agreed that while a business case for HIE can be made, there were concerns about the lack of privacy and security policies, and about the issues surrounding the cost and implementation challenges of HIE. The Payer Sector reported that, with the exception of hospitals, providers in general have made limited investments in the technology necessary to facilitate HIE.

The Workgroup believed that changes in business practices are crucial for HIE, and felt that these changes would initially decrease provider productivity. Implementation of HIE requires new clinical and administrative work processes that would likely not be embraced by most providers.

The Payer Sector agreed that resolving trust issues is crucial to gaining widespread participation in HIE. Consumer skepticism about their sensitive health information being exchanged electronically, as well as issues related to data control, were specifically identified as leading barriers to HIE. Participants believed that consumers must be convinced of the value of HIE, and must be assured that they can control the flow of their information. It was noted that any incidental disclosure of health information could have significant detrimental effects on the adoption of HIE.

2. Workgroup Composition

Participants held senior level positions with state, federal, and private payers, electronic health networks, and a self-insured employer.

The Workgroup included:

Marcia Behlert
Director of Benefits
Constellation Energy

Mike Fierro
Assoc. VP for Healthcare Informatics
CareFirst of Maryland

Sheila Frank
Director, Electronic Information Standards
Delta Dental Plans Association

Sioban McCoy
Director of Payer Sales
Payerpath, Inc.

Alan Shugart
CMS State Programs

Craig Smalls
Director of Operations
Maryland Medicaid

Eileen Giardina
Vice President, Quality Management & Preventation
United Healthcare Mid-Atlantic

Gary White
Director of Operations
Kodak Dental Systems

Robin Kingston
Director, National Sales
Emdeon Business Services

3. State of the Sector in Maryland

The Payer Sector currently has systems in place that support the exchange of administrative health care transactions, which has been occurring since the 1980's. This sector is well positioned to expand its technology infrastructure to support the exchange of clinical information. However, participants noted that modifying systems to support HIE would require a significant amount of time and expense.

4. Sector Readiness for Health Information Exchange

The Payer Sector currently exchanges HIPAA administrative health care transactions with providers, and are evaluating the technical requirements needed to support the exchange of clinical information. Participants felt that by resolving barriers to administrative transactions in prior years, they could anticipate many of the technical challenges they will encounter in exchanging clinical data. The Workgroup had varying ideas as to what data they would likely make available for HIE, but everyone agreed that it would be better to build an exchange incrementally.

5. Current Privacy and Security Practices

The Workgroup reported implementing strict policies regarding user authentication, authorization, access, and privacy and security, and believed that existing policies are adequate for limited HIE. The Payer Sector would like to see statewide HIE policies that build upon HIPAA privacy and security regulations.

Participants reported that their organizations use internal and external auditors to objectively examine, evaluate, and report on the adequacy of system controls. They viewed system audits as a key control mechanism. Annual third party audits include a review of information system internal security procedures, documentation of risk analysis, and adequacy of business continuity plans. These audits typically determine whether appropriate security policies, employee training programs, internal audit procedures, and reporting of security incidents are in place.

a. Authentication procedures

The Payer Sector said their organizations use single-factor authentication, and identified user-based access as the primary method of authentication for employee access to information systems. Individuals are provided with unique user IDs that correspond to specific functions within information systems. Individuals typically select a password that is a minimum of eight characters, with passwords expiring between 90 and 180 days.

Access to sensitive data is also determined by role-based access. Participants noted that sensitive patient information is segregated from other data in their information systems, and is restricted to employees with designated access rights. Sensitive data includes information about famous people, employees, psychiatric treatment, substance abuse, and HIV status.

The Workgroup reported slight variation in the way their organizations authenticate individuals. When members make an inquiry, they are authenticated by answering a series of questions, which may include member identification number, address, date of birth, and other information. Providers are authenticated in several ways, depending on the type of information they wish to access, including provider ID, patient membership information, or claim number. Payers that have implemented web-based provider inquiry functions usually have a separate provider registration process for accessing patient information using the Internet.

b. Method for tracking medical record access

The Payer Sector reported having a designated management-level employee as their HIPAA Security Officer whose duties include completing organizational risk assessments, making security recommendations, and executing audits that enforce security policies and procedures. The use of audit trails is the primary method utilized to track information system access. Participants have procedures in place to monitor and review audit logs on a regular basis. They also reported that audit logs are often extremely large; they are sampled randomly, or at the request of management. Audit logs are manually reviewed and require a significant amount of human resources.

c. Provisions for member access to information

The Workgroup stated that their organizations do not provide their members with access to information electronically. Paper-based reports are provided when a member requests information for legitimate purposes, such as legal requests. Availability of member information through a payer-based web portal or PHR is either limited or non-existent. The Payer Sector noted that detailed policies are in place for family caregivers to access PHI.

d. Member consent

As part of the enrollment process, members typically provide consent for treatment, payment, and health care operations. The Payer Sector reported that members typically do not understand which PHI is routinely disclosed or the circumstances that permit its disclosure. Participants noted that most members do not understand that payers are allowed to use and disclose PHI for purposes related to business operations.

e. Administrative and physical security safeguards

The Payer Sector has made large financial investments in technology and associated infrastructure. Their data centers are in highly secure, climate-controlled environments, which are typically isolated from administrative work areas. Almost all data centers are at off-site locations, and are also used as the communication focal point for the organization. Entry to the data center requires two-factor authentication.

6. Benefits, Barriers, and Risks of Health Information Exchange

a. Benefits

The Workgroup believed that the benefits of HIE are far reaching, but rejected the notion that benefits accrue primarily to payers. They identified cost reduction as the primary benefit of HIE, and said that reducing duplicate testing will dramatically impact health care costs. Improvements in the quality of care and patient outcomes were also identified as benefits of HIE. Participants did not feel that HIE would have a dramatic affect on saving lives and reducing medical errors.

There was considerable discussion about the belief that HIE is valuable to consumers versus the reality that HIE is unproven and its benefits difficult to quantify. The Payer Sector pointed out that they are in the business of managing risk, delivery of care, and cost, and that they hoped HIE would reduce costs and improve the quality of care.

b. Barriers

While the concept of HIE is supported by the Workgroup, skepticism existed about the overall value proposition. Participants viewed the technology required to support HIE as expensive to procure and maintain. The Workgroup felt that payers are more technologically sophisticated than many of the other Sector Groups, and noted that investing in new systems would be difficult to justify, given the length of time necessary to realize an appropriate return on investment. Participants supported the concept of an exchange, but expressed uncertainty about whether investing in a statewide HIE would be a wise decision at this time.

The Payer Sector agreed that the lack of policies related to privacy and security are huge obstacles for advancing HIE in Maryland, and that policy needs to be developed to address the issues of liability and secondary use of data. Any attempt to establish a statewide HIE will require strong public/private partnerships with all stakeholders having equal weight. Concern was expressed regarding achieving balanced consumer representation in a governance structure. Participants agreed that it would be challenging to find individuals who can adequately represent all the diverse consumer perspectives.

Trust in an HIE was identified as an important issue. Participants believed that trust agreements could be used to establish the framework for HIE, and noted that sound trust arrangements need to be a part of HIE policy and agreed to by all stakeholders. Absent sound trust agreements, the Workgroup felt that providers would not be inclined to participate in HIE.

7. Payer Sector Proposed Solutions

a. Require provider adoption of EHRs and e-prescribing.

b. Conduct an environmental scan of payer technology and assess the impact of integrating with an HIE.

c. Include government and non-government payers on any HIE governance structure.

Pharmacy Sector

1. Synopsis

The Pharmacy Sector Workgroup (Pharmacy Sector or Workgroup) included pharmacists with experience working in hospitals, long term care facilities, and independent and chain drug stores. Participants noted that most hospital and long term care pharmacies trail independent and chain drug stores in their use of information technology. The Workgroup reported that nearly all pharmacies use some sort of technology to receive prescriptions, verify eligibility, submit claims, and fill prescriptions. Participants supported HIE and agreed that statewide policy related to privacy and security, access, authentication, and authorization should be developed before patient information is shared electronically.

Physician reluctance to use electronic prescribing (e-prescribing) was identified as a leading barrier to HIE by the Workgroup. Participants agreed that HIE can create efficiencies and improve patient safety, and that eliminating paper prescriptions could reduce the risk of misinterpretation of handwritten prescriptions, and expedite the process of filling prescriptions. For the most part, pharmacies have policies and business practices in place to guard against inappropriate use and disclosure of health information.

The Workgroup mentioned that consumer fear regarding exchanging electronic patient information needs to be addressed. Consumers are concerned about unauthorized access to their medication history by both employers and payers. Patients who are likely to have greater concerns include those taking drugs for the treatment of depression, other psychological disorders, or other diseases to which social stigma is attached, such as HIV/AIDS.

2. Workgroup Composition

The Workgroup had experience in multiple pharmacy settings, and many held senior level positions within their organizations.

The Workgroup included:

Arnold Clayman
Maryland Chapter
American Society of Consultant Pharmacists

Mark Levi
President
Maryland State Board of Pharmacy

Matthew Shimoda
Regional Director
CVS

Shelly Spiro
President
R. Spiro Consulting

Angelo Voxakis
President/CEO
Epic Pharmacies

Stephen Wienner
Owner
Mount Vernon Pharmacy

3. State of the Sector in Maryland

The Pharmacy Sector has a long history of using technology for administrative transactions, such as electronic claims and eligibility inquiries. However, the degree of sophistication varies among pharmacies. The Workgroup noted that some pharmacies have technology in place that supports e-prescribing, while others use technology only to submit claims and verify patient eligibility. The Workgroup reported that independent and chain pharmacies tend to be more sophisticated in their use of technology, compared to long term care or hospital pharmacies. Participants agreed that exchanging clinical information will require almost all pharmacies to retool their current systems. Concerns were expressed about the cost of implementing HIE, as well as the length of time it may take before a return on investment can be realized, both monetarily and through operating efficiencies.

The Workgroup indicated that HIPAA privacy and security protections are not strong enough to handle clinical information exchange, and that additional patient information protections will be needed. Participants also believed that statewide privacy and security policies should be developed before implementation of HIE.

4. Sector Readiness for Health Information Exchange

The Pharmacy Sector reported that most independent and chain pharmacies rely heavily on technology as part of their normal business processes, and support a variety of administrative functions. They also indicated that they would like paper prescriptions to be eliminated. Everyone viewed e-prescribing as a logical first step toward HIE. Through the use of e-prescribing, pharmacies can obtain eligibility information, formulary status, and patient medication history. Pharmacies typically receive an electronic prescription in a few seconds, as compared to the length of time it takes to receive a fax or paper copy. The Workgroup noted that business practices and state laws are viewed as a leading barrier to more widespread adoption of e-prescribing.

The Pharmacy Sector indicated that most long term care pharmacies request prescriptions using a manual and time-consuming paper process. Physicians typically place an order for medication in the medical record, nurses forward a copy of the request for medication via fax to the pharmacy, and the order is filled and delivered, usually on the same day. Participants said that many hospital pharmacies receive handwritten physician medication orders because the hospital lacks a computerized physician order entry system (CPOE). Participants viewed these transcribed handwritten orders as inefficient and prone to error.

The Workgroup believed that the pharmacy sector is more advanced than most other Sector Groups in their use of technology. Participants were enthused about the possibilities of HIE, but had concerns regarding the potential for inappropriate use and disclosure of electronic PHI without strong privacy and security policies.

5. Current Privacy and Security Practices

The Pharmacy Sector reported compliance with the HIPAA Privacy Rule and Security Rule, and felt that HIPAA has helped pharmacies bolster their privacy and security policies and business practices. However, many participants noted that the sector has always strived to maintain strong policies to protect the confidentiality of patient information. Pharmacists spend a considerable amount of time educating consumers on HIPAA. The Workgroup believed HIPAA should be used as foundation standards for statewide HIE.

a. Authentication procedures

Participants pointed out that most pharmacies are small organizations with small staffs. The Pharmacy Sector believed that single factor authentication is sufficient to protect electronic PHI, and mentioned that remote access to pharmacy systems is not widely used. Participants agreed that a business case does not currently exist to provide pharmacists with remote access to pharmacy data.

The Workgroup reported variation in the way providers are authenticated. Authentication can be based on voice recognition, facsimile, call backs, and signature validation. Consumers are authenticated using identity matching questions, or payer or government-issued identification cards.

b. Method for tracking medical record access

Participants noted that most pharmacy systems lack the ability to produce user access audit logs. However, participants indicated that their organizations use well-established processes to track paper and electronic prescriptions. The Workgroup reported that paper prescriptions are kept on file between two and five years, some independent pharmacies keep paper prescriptions for about seven years, and most pharmacies maintain electronic backup copies for about five years.

c. Provisions for member access to information

The Workgroup stated that their organizations do not provide consumers with direct access to their electronic PHI. Upon authentication, patients are provided with a hardcopy of prescriptions filled.

d. Member consent

The Workgroup noted that consent to fill prescriptions is obtained from consumers at the time of purchase. Electronic or paper prescriptions are filled, and as part of the final transaction, consumers sign a form acknowledging receipt of the medication.

e. Administrative and physical security safeguards

The Pharmacy Sector reported using sound business practices to safeguard PHI. Nearly all pharmacies secure medication, paper, and technology behind a locked barrier during non-operation hours. During hours of operation, only a minimal amount of PHI is accessible at any given time. Participants stated that most PHI is maintained electronically, and noted that e-prescribing will eventually eliminate paper records in pharmacies.

6. Benefits, Barriers & Risks of Health Information Exchange

The Workgroup agreed that a statewide HIE would result in significant quality and safety improvements. Participants felt that HIE benefits accrue to payers, and that provider funding for HIE implementation should be included in payer reimbursement. Participants felt that prescribers should be required to adopt e-prescribing. The Center for Information Technology Leadership estimates that e-prescribing could eliminate nearly 2.1 million adverse drug events (ADEs) annually, or an estimated two–thirds of ADEs in ambulatory settings.[32] Several participants emphasized that improvements in patient safety are compelling reasons to justify payers supplementing the cost of technology adoption.

Most participants reported that the greatest single barrier to more widespread use of HIE was the reluctance of providers, not only to invest in technology, but also to take advantage of its capabilities. This reluctance can be attributed to the financial investment required to acquire technology, and the general desire to maintain existing workflow patterns. Participants believed that the State should mandate e-prescibing within the next two years.

The literature suggests that CPOE adoption in hospitals is often slowed by physician resistance, which hospitals frequently cite as the principal reason for non-adoption.[33] In a widely publicized incident reported in 2003, physicians at Cedars Sinai Hospital in Los Angeles forced the hospital to suspend implementation of CPOE due to perceived problems with the system, and workflow disruption issues.[34] The Workgroup pointed out that while provider reluctance to use technology is a barrier, they anticipate that this will change as younger providers more comfortable with technology enter the practice of health care.

7. Pharmacy Sector Proposed Solutions

a. Require prescribing providers to adopt e-prescribing within two years.

b. Include the Pharmacy Sector in discussions aimed at establishing statewide privacy and security policies.

c. Develop strategies to increase the use of technology in long term care and hospital pharmacies.

[32] The Center for Information Technology Leadership, *Patient Safety in the Physician Office, Assessing the Value of Ambulatory CPOE*, (California Healthcare Foundation, April 2004). www.chcf.org/documents/ihealth/PatientSafetyInPhysiciansOfficeACPOE.pdf.

[33] Eric G. Poon, et al., "Overcoming Barriers to Adopting and Implementing Computerized Physician Order Entry Systems in U.S. Hospitals*," Health Affairs* 23, No. 4 (2004), 189.

[34] Laura Gater, "CPOE---Building Electronic Safeguards," *Radiology Today* Vol. 6, No. 12 (June 13, 2005), 18.

Physician Sector

1. Synopsis

The Physician Sector Workgroup (Physician Sector or Workgroup) represented physicians employed by hospitals, as well as physicians in family care, specialty care, and multi-specialty care practices. The Workgroup also included representation from MedChi, the Maryland State Medical Society.

The Physician Sector identified cost as the primary barrier to technology adoption. The Workgroup felt that variation in technology often limits physician adoption. Participants said that technology adoption dramatically changes workflow and business processes, and the learning curve and strain of implementation frequently accounts for physician reluctance to implement technology.

The Workgroup expressed concern regarding data ownership in HIE. Participants are worried that exchanging PHI electronically will increase their malpractice liability exposure. They also expressed concerns about data disclosure. The Physician Sector is aware that consumers are increasingly concerned about who controls PHI stored on paper, and are particularly concerned about safeguarding super-confidential information, e.g., data on psychiatric treatment, substance abuse, HIV, abortion, paternity, or famous persons. The Workgroup believed that HIPAA and State law addresses these issues, but felt that many patients would have concerns about exchanging their health information electronically.

Participants identified lack of trust in payers as a barrier to HIE. The Physician Sector believed that payers will use their data to limit or deny reimbursement, and fear that post payment review of data, which occurs today on a random basis, would become routine in an HIE. The Workgroup noted that payers would likely use data from an HIE as additional leverage in contractual payment negotiations.

The Physician Sector stated that variation in business practices regarding HIPAA and the Maryland Confidentiality of Medical Records Act (MCMRA) present challenges for a statewide HIE. However, participants expressed support for hospital system exchanges, and view connecting physicians to hospitals for limited HIE as a positive first step toward a statewide exchange.

2. Workgroup Composition

The Workgroup included:

Jama Allers
Practice Consultant
MedChi The MD State Medical Society

Ellen Maltz
Practice Consultant
Montgomery County Medical Society

John Lessner, J.D.
Principal, Health Law Group
Ober Kaler

Paul McClelland, M.D.
Psychiatrist
St. Agnes Hospital

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

Mike Gloth, M.D.
Immediate Past President
Baltimore City Medical Society

Larry Gourdine
Health Improvement Network

Ron Haselnus
Practice Administrator
Chesapeake Eye Center

Chuck Henck
Chief Information Officer
University Physicians, Inc.

Joan Irvine
Practice Administrator
Montgomery Internal Medicine Assoc.

Ray Islan
Chief Operating Officer
Darnell Associates, Inc.

Stephen H. Johnson, J.D.
General Counsel, Director of Law and
Advocacy Division
MedChi The MD State Medical Society

Andrew Kundrat, M.D.
Medical Director
Hebrew Home of Greater Washington

Mercy Obamogie, M.D.
Physician
Joel Ogbonna
Catonsville Diagnostic Imaging

Sally Seiler
Chief Executive Officer
The Neurology Center

Michael Tooke, M.D., FACP
Chief Medical Officer
Delmarva Foundation

April Tweedt, DO
Montgomery Family Practice

Robert Wack, M.D.
Physician
Access Carroll

Rick Walker, M.D.
President-Elect
Harford County Medical Society

Linda Whitby, M.D.
Physician

Mark Wiggins
Chief Operating Officer
RxNt

3. State of the Sector in Maryland

The Physician Sector noted that despite the perceived benefits of technology, physician adoption has been slow. In a 2006 study, the Robert Wood Johnson Foundation reported that while 23.9 percent of physicians nationally are estimated to have some form of EHR, only 9.3 percent use EHRs that meet a level of functionality, which allows for meaningful exchange of patient data. The Workgroup believed that the average cost of an EHR, about $33,000 per physician, is a deterrent to adoption.[35] Concern was also expressed regarding

[35] Agency for Healthcare Research and Quality, *Research Finds Low Electronic Health Record Adoption Rates for Physician Groups*, in Press Release (Rockville, MD: U.S. Department of Health and Human Services, September 14, 2005), 2.

work and cash flow disruption during initial implementation, which has been demonstrated to be extensive,[36] and some physicians fear obsolescence of EHR systems. These fears are compounded by uncertainty about the return on investment, and many physicians are unconvinced that a business case to adopt technology has been made.[37]

4. Sector Readiness for Health Information Exchange

The Physician Sector noted that most physicians currently exchange electronic administrative transactions with payers, primarily claim transactions. In Maryland, the percentage of claims that physicians submitted electronically in 2005 was approximately 92 percent for Medicare, 91 percent for Medicaid, and 67 percent for Medicaid Managed Care Organizations and private payers.[38] Participants noted that payers have not fully implemented many of the other administrative transactions, and that it has been an arduous process simply getting to the current level of exchange.

According to the Workgroup, some practices have been able to access hospital information systems via hospital web-based portals. Information available to physicians through these portals includes discharge summaries, medication lists, and lab and radiology results. The Workgroup reported that practices are often hesitant to invest in technology beyond a practice management system, which is used for administrative functions. Many are waiting for technology costs to decrease, or until more is known about statewide HIE.

5. Current Privacy and Security Practices

The Workgroup believed that nearly all practices have written privacy and security policies that are compliant with the HIPAA. Participants noted inconsistency in business practices relating to the interpretation and implementation of HIPAA, but agree that HIPAA has bolstered physician awareness of the importance of privacy and security.

The Physician Sector pointed out that protecting electronic patient information can be difficult, particularly for smaller practices. Participants noted that privacy and security protections are driven by the capabilities of vendor products. Some vendor products are designed to support high levels of privacy and security, while others have more limited protections.

a. Authentication procedures

The Workgroup reported a wide range of security practices in use today. Participants agreed that some practices still do not require authentication of users. Some practices require user name and password and only a few participants were aware of practices that require more information to access the system. The Workgroup had mixed views regarding the appropriate level of user authentication.

The Physician Sector reported that patients are authenticated at the initial office visit, and many participants reported making copies of government or payer issued

[36] Robert H. Miller and Ida Sim, “Physicians’ Use of Electronic Medical Records: Barriers and Solutions,” *Health Affairs*, 23, No. 2 (2004), 118.
[37] Statement of Dr. Peter Basch before the U.S. Senate Commerce Committee, Subcommittee on Technology, Innovation, and Competitiveness, June 30, 2005, http://commerce.senate.gov/pdf/basch.pdf.
[38] The Maryland Health Care Commission collects electronic health care transaction census data from payers on an annual basis as required by COMAR 10.25.09.

identification cards. The Workgroup expressed some concern about methods for absolute patient authentication, and said that office staff typically uses a combination of techniques to identify patients, absent clear identity matching. Participants said that a statewide HIE will need to carefully consider the issue of patient authentication.

b. Method for tracking medical record access

The Workgroup said that most practices do not use audit logs to track user access to electronic PHI, and noted that only academic medical practices would have the technology and resources to review audit logs. Participants noted that most practices rely on employee training to minimize the potential for employees to randomly or inappropriately access PHI.

c. Provisions for member access to information

The Physician Sector does not provide consumers with access to electronic PHI. Participants believed that most physician practices do not have the technology in place to support consumer requests for electronic PHI. They also noted that patients can purchase copies of their medical records for a nominal fee, after authentication.

d. Member consent

The Workgroup noted that patients provide consent to treat through forms completed during registration. They felt that patient consent to participate in a statewide HIE grants permission to disclose PHI, which differs from the consent to treat. While participants believed that they own their patient records, they recognized that ownership of electronic PHI should belong to the patient.

The Physician Sector believed that patients should be able to opt-in to an exchange, and be the only ones able to unlock their PHI. However, the Workgroup agreed that an opt-in model for an exchange would limit access to electronic PHI in emergency situations.

e. Administrative and physical security safeguards

The Workgroup had mixed views on the level of security currently existing in physician offices. They agreed that large practices have been more thorough in their implementation of security measures than small practices. Everyone felt that the level of security safeguards established in practices adequately addresses the risk of intrusion.

6. Benefits, Barriers, and Risks of Health Information Exchange

The Physician Sector ranked improvements in efficiency and quality of care as providing the greatest benefit of HIE. The Workgroup agreed with key findings of the Government Accountability Office, which in 2003 cited 13 specific cost-saving examples resulting from the use of technology.[39] Participants felt that implementation of HIE would accelerate the adoption of new treatment guidelines through the widespread use of clinical decision support applications. Participants noted that implementation of a statewide HIE would

[39] U.S. General Accounting Office, “Information Technology: Benefits Realized for Selected Health Care Functions,” (Washington, D.C.: GAO-04-224, October 2003). http://www.gao.gov/new.items/d04224.pdf. Effective July 7, 2004, the U.S. General Accounting Office’s legal name changed to the Government Accountability Office.

require creation of a significant public/private partnership. The Workgroup viewed the lack of statewide privacy and security policies as a barrier to a statewide HIE.

The Workgroup was concerned that HIE will increase malpractice liability as a result of inappropriate disclosures of data, e.g., sending the wrong chart to the wrong person. They noted that the complexity of patient information access policies increases with HIE, and issues regarding secondary use and disclosure present significant challenges. The Physician Sector also expressed concern regarding the extent that consumers could modify their own health information in an HIE.

Participants reported a lack of trust about sharing patient information with payers. They believed that payers derive the benefits from HIE, and were concerned whether physician data might actually be used to lower their reimbursement.

7. Physician Sector Proposed Solutions

a. Provide physician incentives to adopt technology that includes reimbursement for lost revenue during implementation.

b. Develop an HIE that facilitates physician access to and use of PHI.

c. Establish an HIE that requires patient participation on an opt-in basis.

d. Require hospital systems to electronically connect with service area providers.

Purchaser Sector

1. Synopsis

The Purchaser Sector Workgroup (Purchaser Sector or Workgroup) included individuals from large and small employers, payers, a third party administrator (TPA), a hospital, retirement community, an electronic health network, and a human resources consulting firm. Participants agreed that purchasers are among the principal beneficiaries of HIE. However, they felt that benefits related to HIE would vary among purchasers and require years before they are realized.

The Workgroup agreed that the most significant barrier to implementing an HIE is cost. Participants stated that privacy and security issues need to be resolved before consumers will trust having their health information exchanged electronically, and believed that protecting the privacy and security of electronic PHI is critical to the success of HIE.

Most participants were uncertain of their level of participation in HIE. The Purchaser Sector said they have limited access to administrative information during the insurance enrollment process. They noted that employers that self-insure have access to employee PHI and are considered covered entities and must comply with HIPAA regulations.

2. Workgroup Composition

Participants held senior positions within their organizations and were fairly knowledgeable about issues relating to privacy and security, and the challenges and potential promise of HIE.

The Workgroup included:

Colette Baker
Senior Manager, Employee Benefits
Frederick County Public Schools

Marcia Behlert
Director of Benefits
Constellation Energy

Janet Butler
Data Analysis Manager
United Healthcare

Kathy Clark
Office Manager
Ginger Cove Retirement Community

Robin Kingston
Vice President, Payer Sales
Emdeon Systems

Nisha Madhavan, BSN, CCRN
Chief Operations Officer
Southern Maryland Hospital Center

Julie Perry
Director of Human Resources
Ginger Cove Retirement Community

Elizabeth Sammis, Ph.D.
Director, Government Affairs
Mid-Atlantic Region
United Healthcare

Brian England
President
British American Auto Care, Inc.

Chris Ehrhardt
Director of Corporate IT Administration
Kelly and Associates

John Hulen
Senior VP, Information Technology
United Healthcare

Phyllis Johns Smith
Director
Assisted Living/HIPAA Compliance
Ginger Cove Retirement Community

Deborah Stallings, PHR
President and CEO
HR Anew

3. State of the Sector in Maryland

The Workgroup reported little exposure to administrative health care transactions other than enrollment and premium payments exchanged with payers. The Workgroup felt that at some point in the future, HIE would allow purchasers access to information that could be used to develop employee wellness and education programs.

4. Sector Readiness for Health Information Exchange

Some participants reported that they are currently exchanging administrative health care transactions electronically with payers. Participants of the Workgroup believed that any increased use in technology would be well received by purchasers. They noted that self-insured employers are further along in their use of technology for health care transactions than some of the others in the sector.

Participants believed that adoption of HIE could increase purchaser costs. The Workgroup said that technology use varies by industry and that few purchasers today are prepared to participate in HIE. They felt that technology implementation will require adopters to have a clear understanding of its value. Participants compared adoption of HIE to the introduction of the Internet, which has brought value to most sectors.

5. Current Privacy and Security Practices

There is considerable consumer anxiety regarding Purchaser Sector access to employee medical information. In a recent survey, 52 percent of respondents voiced concerns about employer misuse of insurance claim information.[40] HIPAA prohibits the unauthorized disclosure of individually identifiable health information by covered entities except as necessary for treatment, payment, or health care operations. Self-insured employers are considered hybrid entities under HIPAA. These entities use or disclose PHI for only part of their business operations, which are covered by HIPAA regulations.[41]

[40] "National Consumer Health Privacy Survey, Survey 2005." (California HealthCare Foundation, November 9, 2005), 15. http://www.chcf.org/documents/ihealth/ConsumerPrivacy2005Slides.pdf.

[41] 45 CFR 164.504.

The Workgroup was concerned about the ability to adequately safeguard health information in electronic formats. Participants agreed that nearly all purchasers currently have some access to PHI, and that business rules, more than policy, dictate how it is accessed, used, and disclosed. Participants agreed that absent statewide policy, patient information is at a high level of risk for disclosure, whether it is maintained electronically or on paper.

The Workgroup believed that stronger protections are required before a business case can be made to implement HIE, and agreed that privacy and security is a key issue that needs to be addressed. Participants noted one incident where the lack of stringent policies may have been a factor in the loss of data tapes containing personal and financial information for 135,000 patients, employees, and retirees.[42]

The Purchaser Sector reported compliance with the HIPAA Privacy Rule and Security Rule when acting as a self-insurer for health care, although most purchasers are not covered entities. Purchasers that are covered entities reported familiarity with HIPAA requirements.

a. Authentication procedures

Participants said they employ user name and password to access systems containing PHI. Self-insured purchasers partition systems with PHI from other data. Users are granted role-based access to the system.

b. Provisions for member access to information

Participants said that employees do not have electronic access to PHI. Employees that request health information maintained by the organization are provided with a paper copy.

c. Administrative and physical security safeguards

The Workgroup felt that they have adequate measures in place to safeguard PHI. Self-insured employers noted that paper records related to health care are kept separate from employee personnel files, and are locked at all times.

6. Benefits, Barriers, and Risks of Health Information Exchange

The Workgroup could not reach consensus on the short-term benefits of HIE. Participants felt that HIE would initially add to existing business costs, but could provide some measurable long-term value.[43] Nearly everyone agreed that HIE increases the risk of unintended disclosures, and that it could take at least one or more years to develop and implement appropriate privacy and security policies. They also believed that adoption incentives would help promote HIE.[44]

[42] Susan Kinzie, “Lost Computer Tapes Had Details on 135,000 Workers, Patients,*” Washington Post*, February 7, 2007, Sec B, p 5.

[43] Francois deBrantes, et al., “Financial Incentives for Adoption of Health Information Technology by Healthcare Deliverers,” *US Healthcare Strategies*, 2005. http://www.touchbriefings.com/pdf/1251/deBrantes.pdf.

[44] Glenn Hackbarth and Karen Milgate, **“**Using Quality Incentives to Drive Physician Adoption of Health Information Technology,*” Health Affairs*, 24, No. 5 (2005), 1147.

7. Purchaser Sector Proposed Solutions

a. Develop incentives for self-insured purchasers to adopt health information technology.

b. Identify the short-term benefits of HIE for self-insured purchasers.

Recommendations & Next Steps

1. Recommendations

Privacy and security issues pose challenges to electronic health information exchange (HIE). Eight Sector Groups -- consumer, hospital, medical laboratory and diagnostic imaging centers, long term care, payer, pharmacy, physician, and purchaser -- agreed that establishing strong privacy and security protections is paramount to the success of HIE. MHCC's assessment of privacy and security focused on business policies and practices in general, and security policies and practices in particular, that may hinder the development of HIE in Maryland. Lessons learned from the assessment will help facilitate efforts to develop solutions and implementation plans that span across all Sector Groups for statewide data sharing.

The following recommendations are based on the work of the eight Sector Groups:

Develop statewide policies to address access, authorization, authentication, and privacy and security of electronic health information.

Sector Groups agreed that sound policy must be established before patient information can be exchanged electronically. Most participants were of the opinion that technology has outpaced policy, and that trust in any system of data sharing can only be established through sound policy. Participants felt that absent statewide policy, patient information will remain locked in information silos that are maintained individually by the provider community.

Resolve issues relating to ownership and control of electronic health information.

Sector Groups expressed mixed views about ownership of electronic health information. Participants had concerns regarding the risks of secondary disclosure of electronic health information, which can increase in an electronic environment. Some participants believed that regardless of the data sharing model, it is critical to notify consumers when their information is accessed.

Encourage hospital systems to foster development of data sharing with service area providers.

Sector Groups believed that data sharing needs to begin within each hospital system. Participants viewed data sharing within a hospital system as a logical first step to developing statewide electronic health information exchange. Almost everyone agreed that while hospital systems are better suited to work through technology barriers, they are not very well-equipped to develop exchange policies.

Move forward in developing statewide electronic health information exchange.

Sector Groups universally agreed that a statewide system for exchanging patient information would improve health care quality and increase efficiency in health care. Some participants had concerns about moving too quickly to implement a data sharing system, however, most participants thought that planning should begin for implementation of statewide HIE. Resolving privacy and security policy issues is a leading concern among Sector Groups.

Develop consumer education initiatives relating to electronic health information exchange.

Sector Groups considered consumer education essential to building trust in an exchange. Participants believed that consumers have mixed views about sharing patient information electronically. Overall, participants felt that consumer trust does not extend beyond their own physicians. Participants believed that providing consumers with information on the value of sharing patient information electronically will significantly reduce anxieties related to HIE.

Explore state funding opportunities in the form of grants and small business loans for provider acquisition of health information technology.

Sector Groups agreed that funding opportunities could modestly increase provider investment in health information technology. Most participants had slightly different views regarding the value of provider grants and business loans, but agreed that they could increase technology adoption rates.

Resolve concerns over increased provider liability with electronic health information.

Sector Groups were concerned about the increased provider liability related to HIE. Nearly all providers felt that having access to additional patient information will increase malpractice claims. Providers were generally unclear whether electronic patient information increases physician duty or liability.

Develop a standard set of data that can be used for sharing information within a hospital system and in an exchange.

Sector Groups agreed that a standard set of data needs to be identified for use within a hospital system exchange. Participants believed that identifying a core set of data will be useful to hospital systems as they implement data sharing. Most participants thought that a more limited set of data should be developed for a statewide HIE.

Determine data uses for purposes other than treatment, payment, or health care operations.

Sector Groups believed that secondary disclosure of electronic patient information needs to be addressed. Participants viewed redisclosure as an area of concern that can be addressed through establishing trust hierarchies. Participants also believed that data can be adequately de-identified and used for other purposes.

Consider the broad impact of personal health record adoption on electronic health information exchange.

Sector Groups thought that consumers can be more engaged in managing their health care through the use of personal health records (PHRs). Participants believed that the value of PHRs stems from their ability to store patient information and, in the near future, to respond to what is happening in patients' daily lives, rather than being a static repository of their health information.

Develop legislation that includes incentives for health information technology adoption, and explore the impact of mandating its use by 2014.

Sector Groups were somewhat cautious about recommending that the State legislate health information technology (HIT) adoption, however, almost everyone agreed that legislation will promote widespread technology adoption. Many participants felt that mandating HIT adoption should be considered at a future date.

2. Next Steps

As the final step in this assessment, MHCC convened a group of stakeholders representing the eight Sector Groups to craft preliminary solutions and implementation plans that could be used for further deliberation by a Solutions and Implementation Workgroup. The State will assemble a diverse workgroup, using the recommendations from this initiative, to develop solutions and implementation plans for privacy and security policies and business practices as they relate to sharing health information electronically.

The MHCC and Health Services Cost Review Commission (HSCRC) plan to release a Request for Application (RFA) to fund up to three planning projects for a statewide HIE in the fourth quarter of 2007. The work of the Sector Groups is expected to aid in the development of a strategy for phased implementation of a statewide HIE. The results of this assessment, and that of a Solutions and Implementation Workgroup, will provide useful information to the work of the three planning projects.

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

Website: mhcc.maryland.gov
Telephone: (410) 764-3578   Fax: (410) 358-1236