Privacy and Security Solutions for Interoperable Health Information Exchange

Massachusetts HISPC Report
Deliverable No. 5 State Final Assessment of Variation and Analysis of Solutions Report

RTI Subcontract
Project Number 27-321-0209825

March 30, 2007

Prepared by:

Ray Campbell, JD, Diane L. Stone, MBA
Susan A. Miller, JD, Jerilyn W. Heinold, MPH, David S. Szabo, JD
Massachusetts Health Data Consortium As Designated Subcontractor by the Commonwealth of Massachusetts

Submitted to:

Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

Table of Contents

Executive Summary

Several Massachusetts organizations are currently conducting electronic health information exchange (HIE) in the Commonwealth. Private sector organizations have invested significant time and resources in HIE projects that move interoperability forward through both pilot initiatives and production systems.

In the public sector, the Commonwealth of Massachusetts Executive Offices of Health and Human Services (EOHHS) has created a web portal for health and human services programs known as the "Virtual Gateway." The Virtual Gateway is intended to provide a single access point to all EOHHS initiatives for consumers, providers, legislators and researchers.

Based on stakeholder input and Project Team analysis, MA-HISPC identified four (4) issues as key barriers, sources of variations in business practices, or key public policy concerns. The issues are: (1) patient consent to the use of HIE networks, (2) use and disclosure of sensitive medical information, (3) implementation of access controls, and (4) application of community standards.

Based on MA-HISPC analysis of these four key issues, MA-HISPC identified four (4) categories of solutions that, when applied to each type of barrier, will markedly advance HIE in the Commonwealth: Legal, Technical, Policy, and Education. We have identified solutions in each category that will apply to each of these barriers. Additionally, we consistently found that stakeholders manage health information with markedly differing interpretations of HIPAA, other federal laws, and state laws. Thus, a set of solutions is in order around policy development which will support operations and education for the consistent implementation of these laws. Finally, the development and implementation of a comprehensive communication strategy was identified as a critical component of all our future work.

After further consideration of these four barriers, MA-HISPC has now focused its implementation planning on two priority areas: (1) patient consent for the use of HIE networks; and (2) use and disclosure of sensitive health information. We feel that each area must be addressed through legal, technical, policy and educational solutions. At each stage of the work and discussions — VWG, LWG, SWG, and now IPWG — the MA-HISPC project determined that these two areas need to be addressed before true interoperable electronic HIE is possible in Massachusetts. The recommended solutions and implementation plan includes:

<u>Patient Consent:</u>

- Develop a common understanding of state laws and regulations related to patient consent as applied to information networks and HIE
- Ensure that future HIE systems will be able to capture and share patient opt-in and other preferences, capture patient consent at one point in the system and flow this information to all clinicians and clinical points of care, and record and implement changes in consent with changes in patient's medical and clinical conditions
- Establish industry consensus policies and procedures addressing patient consent and sharing of patient consent, to be implemented with a flexible framework across the HIE enterprise, including policies to enable consent at one point of care to appropriately flow to all clinicians and clinical points of care

- Address current and continuing education needs regarding state and federal laws and regulations.

Sensitive Health Information

- Develop common understanding of state and federal laws and regulations related to sensitive health information.
- Need to develop and disseminate uniform definitions of sensitive health information, based on state and federal laws.
- Identify the technical needs for sensitive information management within an EHR and RHIO, along with baseline business and technical policies that must be in place for sensitive information management.
- Ensure that future electronic HIE systems will be implemented with a flexible framework to enable identification and classification of sensitive information within databases, creation of sensitivity flags for use in the EHRs and RHIOs, and the use, when applicable, of data-filtering technologies to filter sensitive information based on state laws and regulations.
- Ensure that future HIE systems will be able to flag sensitive data (general and in a specific patient's electronic records), block external access to internally flagged sensitive data actions, both of which should be coupled with effective communication to system users that some kinds of information may be blocked. In this way clinicians can use the system appropriately with patients.
- Address current and continuing education needs regarding state and federal laws and regulation

The MA-HISPC has developed a preliminary implementation plan that includes use case scenarios and working groups to develop clinical, policy, legal and technology work product. The plan will be shared with communications and education task forces to inform their processes. This work will enable implementation of solutions while we coordinate our work with other states and with national initiatives.

1. Background

1.1 Purpose and Scope of Report

Massachusetts' Final Assessment of Variation and Analysis of Solutions Report (MA-HISPC State Deliverable No. 5) is submitted by the Massachusetts Health Data Consortium, Inc. (MHDC) to RTI pursuant to contract 290-05-0015. MHDC was designated by the Commonwealth of Massachusetts as the Massachusetts Health Information Security and Privacy Collaborative (MA-HISPC) to follow the approved Work Plan and carry out the Project deliverables for the Massachusetts subcontract to RTI # 27-321-0209825. The purpose of this Report is to fulfill the objectives of Deliverables No. 5 and refine and expand upon the two previous interim reports. The MA-HISPC Steering Committee, Variations Working Group (VWG), Solutions Working Group (SWG), Legal Working Group (LWG) and Project Team have fully discussed, reviewed, and expanded their variations and solutions considerations for Massachusetts. The scope of this Report represents a distillation of the broad collection of business practice and barrier information identified by the Variations Work Group, analyzed and

organized into recommended solutions by the Solutions Work Group, and prioritized by importance, logical starting point and feasibility by the Implementation Plan Work Group.

1.2 Description of level of HIT development in the state

The Massachusetts healthcare community has initiated the development of various HIE projects in the last few years. Some are just entering their operational phase. A brief but not comprehensive list:

- MedsInfo-ED – provided real time patient Rx history to pilot emergency departments from multiple health plan and PBM data sources; accomplished community consensus regarding consent management, sensitive information handling, and patient identification.
    - This was a mature HIE project operated on a pilot basis in five hospital EDs
- MA-SHARE Rx gateway – end to end ePrescribing, addressed vendor contracting, patient identification, transactions standards, and sensitive information handling.
    - This is an advanced HIT project now going into production.
- MA-SHARE - clinical data exchange – pull services – addresses record locator services, record publishing services, transaction standards. This project uses technology developed with a Markle grant. It is not currently deployed, but the technology is functional.
    - This is an advanced HIT process.
- Massachusetts eHealth Collaborative (MAeHC)- introducing and providing community-based electronic health records, clinical decision support, and clinical data exchange in all clinical settings; creating community- defined infrastructure, identifying and managing the provider and consumer/patient barriers to adoption including consent management and sensitive information handling.
    - This is an HIE project rapidly growing to the advanced state and being deployed in three communities.
- SafeHealth – pioneering technology that will enable clinicians to appropriately access relevant patient medical information in emergency and ambulatory settings; policies and procedures for consent management, sensitive information management, and more.
    - This is a mid-level of development HIE project.
- Masspro – DOQ-IT, supporting the EHR adoption and implementation – workflow analysis, cultural change.
    - This is an advanced HIE project.
- New England Health EDI Network (NEHEN) – administrative transactions flow between the Massachusetts health plans and large Massachusetts providers.
    - Significantly advanced HIT operation, functioning since 1997 in 30 participating institutions. This may become a platform for other HIE initiatives.

1.3 Description of report limitations

The MA-HISPC Steering Committee, Working Groups and the Project Team considered all the interoperability privacy and security concerns, issues and recommendations from the Variations Working Group and the Solutions Work Group Interim Reports, plus the LWG internal report and outlined the following limitations:

- Interoperable electronic health information exchange (HIE) is growing in Massachusetts, but it is still fragmented, under funded, and seeking viable business models for return on investment.
- The Massachusetts Health Data Consortium is a neutral third party convener with a collaborative structure supporting work in privacy and security. Nonetheless, HIE is still occurring in silos across Massachusetts.
- The work of the four current federal contracts: HITSP, HISPC, NHIN, and CCHIT, highlight the need to develop key standards and policies at a granular level like the work being carried out at the national level by the Health Information Technology Standards Panel ("HITSP"). However, the scenarios and case studies across the four federal contracts are not uniform.
- Working in partnership with other Massachusetts HIE advocates, the dissemination of project experiences as well as policy and procedure work products continue to be well supported goals. However, efficient coordination of specific work products is a challenge when each group may have a different agenda.
- The Massachusetts HIE projects outlined above have accomplished their interoperability goals by focusing on HIE initiatives with limited scope and by following a logical and sequential set of workflow steps. While the Massachusetts HIE projects are technologically and operationally advanced, they are still initial steps that can serve as building blocks to full electronic HIE.

Most importantly, Massachusetts has not yet identified a source of financing to support any recommended action plan from MA-HISPC's implementation work. The MA-HISPC action plan is premised on MHDC moving forward in partnership with the planning and operational experience and work products of the Massachusetts eHealth Collaborative (MAeHC), Masspro, SafeHealth, as well as the Commonwealth of Massachusetts. During the implementation project MA-HISPC will also work with the two large integrated Integrated Delivery Networks (IDNs), Partners Healthcare and CareGroup. All these organizations have developed HIE policies and procedures for their defined healthcare communities, thus allowing operational projects to exchange clinical data. Without commitments to economic support, there will not be a firm foundation upon which to build the next level of HIE in a timely way.

2.0 Assessment of Variation

2.1 Methodology Section

MA-HISPC commenced Work Plan activities by signing RTI's subcontract in May 2006. MA-HISPC Steering Committee was constituted in March 2006 and convened its first scheduled monthly meeting in May. All RTI recommended Stakeholder Group representation was identified and included in Variation Work Group interviews.

<u>Approach</u>

The original Stakeholder Group and Steering Committee approach for business practice data collection and barriers identification assigned each of the 18 scenarios to four stakeholder Variation Work Groups.Given the OMB hold during July 2006 and August 2006, the Steering Committee approved an alternative approach to organizational level business practice data collection and variations analysis. Since the majority of stakeholders had been identified, invited and accepted participation in February 2006 as part of MHDC's RTI RFP submission, the MA-HISPC Project Team was permitted to convene individual Stakeholder interview meetings. Between August 15 and October 18, 2006, over 30 one-to-one stakeholder interviews took place.

Since it was determined that significant subject matter expertise was required to gather valuable privacy, security and health care setting information from the stakeholder interviews, MA-HISPC interviews were conducted by the three primary MHDC Project Team Staff. Most interviews were structured with a Project Team note taker, interviewer, and facilitator. The team used the same script in all interviews to maintain, to the extent possible, uniformity of responses. The script asked what each stakeholder would do in the situation, why they would do it, and on what basis. This process resulted in a description of the relevant workflow, a listing of references to regulations, policies, statutes, case law, common practices believed to be appropriate for the situation, as well as a qualitative discussion on satisfaction, including ease or difficulty with the business practice. Where applicable, stakeholders provided additional information if a business practice is manual today; they considered how the issues would be resolved or created if there were electronic capability.

- The RTI Team review of MA-HISPC's Interim Variation Report suggests that Massachusetts be aware that the [1]one-on-one interviews for the variation report might "hamper cross stakeholder 'buy-in' of solutions." The MA-HISPC project team has not found that the variation data collection process has hindered any stakeholder buy-in or any follow-on HISPC project work, in part because subsequent phases of the project, such as solutions development, have been based on project workgroups and not one-on-one interactions. We have discovered tremendous enthusiasm, interest, and commitment by the stakeholders. The project is now planning to use a number of dedicated email lists and listservs to inform the greater community and gain their comments which will be folded into implementation work planned by the MHDC and the Massachusetts healthcare community. Cross stakeholder feedback and buy-in was also accomplished as part of the LWG, SWG, and IPWG face-to-face meeting time. At least 25% of all subsequent working group discussions were devoted to fine tuning addition of variations, best practices, and barriers.

Data Management

The MA HISPC Project Team managed the data collection and data entry process in a manner that supports the earliest and most effective access to business practice information for quantitative and qualitative review and analysis. The process involved five steps after each interview: meeting note preparation; transfer of that data to spreadsheets for each stakeholder/ scenario, matching the information required for the RTI Assessment Tool; transfer from the

[1] The blue paragraphs, comments and other notes are the MA-HISPC responses requested in the MA-HISPC VWG interim report review and the MA-HISPC SWG interim report review.

Excel spreadsheets to the MHDC-constructed Access Data Base for data manipulation and analysis; and data transfer to the RTI Assessment Tool.

With the majority of stakeholder interviews completed by September 30, 2006, the Project Team needed immediate data base functionality to sort and filter business practices, domains and barriers in order to prepare an agenda and content for the LWG and begin to identify appropriate representation for the SWG. As a result, MHDC staff programmed its own Access Data Base to provide the sorting and display of data required for subsequent project steps and analyses.

Completion of VWG activities

By mid-October 2006, MA-HISPC accomplished its work to fulfill VWG's objective of interviewing and collecting stakeholder current business practices around the RTI scenarios. At its October 11, 2006, meeting, the Steering Committee reviewed the information and accepted the VWG data collection work as complete. With the majority of stakeholder groups represented on the Steering Committee, it was agreed that stakeholder interview activities had reached a point of diminishing returns in terms of additional learning. The Steering Committee thus concluded that VWG's goal of collecting information that is a fair reflection of the current state of health information interchange in Massachusetts had been achieved, and agreed to move ahead with Legal Work Group activities.

MA-HISPC then continued to summarize the data and enter it into Excel spreadsheets and the Access Data Base where it could be sorted to identify a core set of business practices classified by domain and tagged as "barriers." These summaries were forwarded to the LWG.

Legal Working Group (LWG)

The LWG is composed of Executive Office of Health and Human Services (EOHHS) and departmental senior legal representatives from the Commonwealth of Massachusetts, and four private sector attorneys recognized by the local and national healthcare privacy and security community. The LWG developed its mission and charter as well as a required confidentiality agreement. LWG convened three times in October 2006 to identify and address barriers indicated in the 135 business practices. The LWG discussed and identified not only the legal barriers, but provided additional insight to business practice issues and obstacles. The richness of the LWG discussions led the Project Team to customize a spreadsheet (based on another RTI HISPC State initiative) to gather the critical data for this Project and provided a basis for the SWG activities.

Statistical Summary of VWG information Collection

This Report represents the findings and feedback from multiple stakeholder interviews across 18 scenarios to collect organizational level business practices.

Project Statistics	
20	Number of stakeholder types represented
18	Number of scenarios where data was collected
76	Number of MA-HISPC stakeholder to scenario interviews
346	Number business practices collected for the 76 stakeholder/scenario interviews
135	Number business practices identified as barriers -- 39% of all business practices

Report Organization

This summary of relevant findings is presented in the RTI requested format. Further, in each scenario grouping a discussion is provided that separates most frequent domains identified, barriers identified for that domain, followed by reference to applicable business practices. After preliminary review of the data, MA-HISPC categorized the barriers or impediments to interoperability most frequently discussed into eight (8) types listed below. While in some cases two stakeholders identified the same barrier, importantly, the barriers represent information from specific interviewed stakeholders, and are not substantiated statements from any statistically derived, widespread data collection study.

MA-HISPC and the stakeholders felt that it is important to emphasize that some of the laws and business practices limiting health information exchange may—in many cases—be desirable, even if those laws and practices are barriers in some sense of the word. For example, in a city constructed below sea levels, barriers to the free flow of water are good thing. In our work, we have tried to distinguish between unintended barriers (or those that don't offer offsetting benefits) from barriers that may have been created for good reason. Ultimately, policymakers must decide whether barriers should be eliminated, modified, or preserved.

Barrier Categorization developed by MA-HISPC	
Legal	Existing Federal, Massachusetts law and regulations governing use and disclosure of health information
Technical	The inability to electronically transfer data in a secure manner, references the lack or current shortcoming in format compatibility, semantic interoperability, transmission interoperability
Privacy	In some cases, privacy rules, such as the need for consent (under Massachusetts law) or HIPAA authorization, the application of the "minimum necessary use" test – many of the HIPAA requirements are barriers. In other cases, providers may decline to disclose information (even when allowed by applicable privacy rules), due to concerns that the downstream recipients will not protect the patient's privacy. Some privacy barriers may be viewed as appropriate, however, even if they are strong barriers to interoperability.
Cultural	Healthcare staff at covered entities indicates that current procedures to information exchange work fine, are sufficiently timely, and provide accurate data exchange. Thus the need to change is not compelling.
Resource	A covered entity/organization does not have either the personnel or the funds to allocate to electronic HIE initiatives.
Workflow	With training, education, and better capabilities, electronic HIE could occur. (Not just training – but physical rearranging of environments as well.)
Perception	Healthcare staff follow a procedure believing it is driven by a legal requirement; both Massachusetts state law and HIPAA
Security	Current architecture of the technical application does ensure appropriate access controls, authentication, and role-based capabilities. Current manual systems for access control and authentication rely on routine nature of requests and trust factors between individuals and entities

2.2. Summary of Relevant Findings Purposes for Information Exchange

The following section presents information about variations in practice found for the groups of scenarios reviewed with stakeholders. Presented are the domains explored and critical observations about privacy and security standards.

2.3 Treatment (Scenarios 1–4)

2.3.1 Stakeholders

The VWG Project Team interviewed 12 Stakeholder types to collect information on business practices for the first four treatment Scenarios related to health information exchange during patient treatment. Stakeholders represented the following: complex hospital system; community hospital, Commonwealth of Massachusetts EOHHS (including Departments of Mental Health, Transitional Services and Public Health); clinicians; medical society officer; physician medical group medical director; Massachusetts eHealth Collaborative EHR Project; clinicians, consumer

advocate, homeless shelter – community health center; long-term care facility and hospice care; mental health and substance abuse trade association.

2.3.2 Domains

MA-HISPC collected 77 Business Practices for these first four Treatment Scenarios. Barriers to HIE were indicated for 60 business practices involving 8 domains – all but domain number 6: "Information audits that record and monitor the activity of health information systems." In order of frequency, the business practice barriers for Scenarios 1 to 4 were associated with:

Domains	
8	20 (33%*) State law restrictions
9	12 (20%) Information use and disclosure policies that arise as health care entities share clinical health information electronically
1	12 (20%) User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be
4	10 (17%) Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network
2	3 (5%) Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information
7	1 (2%) Administrative or physical security safeguards required to implement a comprehensive security platform for health IT
5	1 (2%) Information protections so that electronic personal health information cannot be improperly modified
3	1 (2%) Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises

***Percents sum to greater than 100 because of rounding.**

Domain and Business Practices Discussion

#8 State law restrictions

◊ Barrier

Legal: Within the four treatment scenarios, Massachusetts law requires consent to share medical data, and it requires a second informed written consent for sensitive data (including mental health information, substance abuse information, HIV information and genetic information), whether the transfer of clinical information is by paper or electronic means. This second informed consent for sensitive data is necessary for each subsequent disclosure (described as "per instance" consent). The protection follows the medical record. Massachusetts consent laws are barriers to the interoperability of electronic medical records.

◊ Business Practices

The business practices relate to three circumstances: initial consent from patient, second consents and handling of sensitive information (HIV, substance abuse, genetics), and transfers of PHI. Of note, one stakeholder summarized the critical nature and basis for consent requirements around sensitive information: "loss of privacy means a person cannot get loans and jobs. The stigma of mental health and substance abuse issues is still tremendous."

#9 Information Use and Disclosure

◊ Barriers

Culture: Phone and fax procedures are seen as appropriate, effective and sufficient, since they capture the richness of the information being exchanged for patient care. They also permit providers to communicate in order to gain nuances not necessarily obvious in an electronic data record. To date, no crisis appears to have occurred. The current system of telephoning other providers for required information works. Providers feel that telephone exchange is good and that changes could adversely affect current efficiency of workflow.

Technical: Work is continuing to standardize CCR (Continuity of Care record) to address minimum necessary. More advanced providers setting policy to not allow any "pulling" of data from their electronic medical record systems, rather will hold the control and "push" requested information after determining appropriateness of the request and a minimum necessary review.

- Technology initiatives find greater acceptance when data exchange occurs within communities; when data is transmitted outside of local communities or across state lines, stakeholders are more likely to "shut-down" data exchange or more rigorously apply the "minimum necessary" rule. Even within technology there is a cultural understanding that privacy practices are inextricably bound up with trust.

- Most consumers think an EHR means that the full paper medical record has been scanned into an electronic file. The concept of Continuity of Care Records (CCR), or a designated record set, is not generally understood.

Perception: Minimum necessary must be applied at each instance of a provider using or disclosing PHI even in treatment settings. However, a HIPAA exception states that minimum necessary is not required for releasing PHI for treatment purposes.

◊ Business Practices

Covered entity request for PHI from another covered entity, in some cases across state lines, is a manual process using telephone and fax machine transmission of information needed for patient care.

Prior to disclosure of PHI, minimum necessary considerations take place, often with each entity applying a minimum necessary consideration, even if not required.

HIPAA's minimum necessary use requirement was a recurring theme in stakeholder interviews. The minimum necessary standards within the privacy rule states:

When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Another recurring theme was versioning of medical records in an electronic data base; for example, at data entry, when reviewed by a clinician with out his/her signature; with his/her signature. Policies and procedures are needed for all versioning types defined within a provider.

The rule contains exceptions to this requirement, and also sets forth detailed steps for implementing the requirement when it does apply. Our findings suggest that this aspect of the HIPAA privacy rule is not well understood.

Domain Number 1 User and entity authentication

◊ Barriers

Security: Since the procedure is currently manual, issues of adequacy of confidential receipt of PHI, and the routine of a call back to verify the requesting entity are appropriate. The use and receipt of PHI are based on trust factors, rather than industry level standards of verification and information protection.

Cultural: Providers in Emergency Departments will accept information on patient from any source without regard to consent or permission.

◊ Business Practices

The business practices relate to the process for authenticated PHI requestor (physician or entity); because this is a manual process, providers use a traditional means of calling back. The expectation is that authentication takes place; there is trust in the system.

2.3.3 Critical Observations

For Solutions Work Group consideration:

- Establishing effective and efficient electronic consent
    - Patients need all forms carefully explained to them. They need to trust the system. Consumer advocate thinks phone is best way to communicate, but that younger patients would accept electronic transmission.
    - After elaborate decision-making about “opt in” or “opt out”, one community elected to use an opt in or patient choice model.
    - If patient does not sign consent, referring physicians will still send the patient to PCP but without any PHI with a note indicating that patient refused.

- Additional acquisition of secondary consents for sensitive information and establishing effective and efficient electronic consent, including issues around the form of consent and the procedure for obtaining consent.
    - It is suggested that education about how information is shared and transmitted could go a long way toward assuring patient trust and consent.
    - EHR requires elaborate filter system throughout the medical record to protect sensitive information
- The ability to transfer part or all of the medical record
    - Technology: currently no import/export mapping with EHR vendors
    - Many providers and consumers tend to have cautious attitudes about the Internet, not yet fully trusting security technology associated with electronic transactions.
    - Versioning: of medical records in an electronic data base; for example, at first preliminary data entry, and then when finalized by a clinician with or without his/her signature. Policies and procedures and standards are needed for all the versioning types defined within a provider.

2.4 Payment (Scenario 5)

2.4.1 Stakeholders

The VWG interviewed seven (7) stakeholder types to collect the business practices and barriers for Scenario number 5, the *Payment scenario* referencing health plan case management activities to approve inpatient hospital stays. Stakeholders approached this scenario with the assumption that the case management was a concurrent review process. Stakeholders represented: complex integrated hospital delivery system; health plan payer; clinician, physician group practice, Federal health agency, long term care nursing home and hospice care; consumer as patient and parent. The assumption was that this is a concurrent review use case, and provider releasing data relies on payer contractual obligations to insured. Stakeholders reviewed this scenario as a payment issue only.

2.4.2 Domains

MA-HISPC collected 30 Business Practices for this Payment Scenario. Barriers to HIE were indicated for seven (7) business practices involving domains number 9 Information use and disclosure policies, 4 business practices (57%) and number 8 State Law restrictions with 2 BPs (29%). The majority of business practices for this scenario were not flagged as barriers to interoperability. If disability insurance was considered for this scenario, access to PHI would require a patient authorization. If EAP [Employee Assistance Program] was considered for this scenario, access to PHI would require a patient authorization.

Domain and Business Practices Discussion

Domain Number 9 Information Use and Disclosure

◊ Barriers

Security: Issues with respect to security domains for access control and audit were raised during the discussion of use and disclosure.

Technical: Requires specific architecture to access selected components of EHR; most applications do not yet have this capability for remote access. In addition, applications that do currently allow access are read-only and require secure remote access security controls and technology.

Legal: There are no serious Massachusetts legal barriers. Consent or authorization for payment is the only review that will need to be considered. Most often the authorization is implied when an individual applies for or accepts health insurance. If consent is not in the insurance agreement then a patient may need to consent to allow disclosure to payer for the medical services that have been provided. Under Massachusetts state law and regulation specific types of sensitive information sharing need specific consent by a patient.

There are no HIPAA barriers since PHI may be used for treatment, payment, and healthcare operations without a written consent by a patient.

Resource: It is unclear who should make the investment in this remote access technology, the provider or the payer. There is substantial cost and providers question Return on Investment (ROI).

◊ Business Practice

The business practices described for a case manager review of patient charts outlined the expectation that minimum necessary requirements would be complied with; however, they cannot be monitored or audited.

2.4.3 Critical Observations

For Solutions Work Group Considerations:

- For minimum necessary, the software applications must address the need to provide access to only the appropriate sections of an EHR, and provide "view only" access. Currently, the paper record access on patient floors has no audit controls.

- Clarify the need for patient consent to permit a health plan payer access to portions of medical record for payment purposes. Stakeholder interviews and the LWG analysis suggested that various providers and payers have differing views on key state law issues. For example, some payers have interpreted HIPAA to explicitly permit them access to PHI for payment purposes and have removed the consent portion from the health plan enrollment form. Our work disclosed varying interpretations of state law regarding the need for express patient consent prior to uses of protected health information for treatment, payment, and healthcare operations. Health plans take the position that legal permission to disclose PHI is implied when an individual applies for or accepts health insurance. From a provider's perspective, if consent is not explicitly contained in the insurance agreement then a patient

will need to consent to the use of protected health information for payment of medical services that have been provided.

- Consumer expects: minimum necessary, verification of a person's access, and expects that there are laws governing this. Consumers do not differentiate between paper or electronic record. They think electronic may be better since it would be more efficient.

- If a secure portal was available to health centers and clinics, these providers would want an arrangement through a gateway to the health plans.

2.5 RHIO (Scenario 6)

2.5.1 Stakeholders

The VWG interviewed ten (10) stakeholder types to collect the business practices and barriers for Scenario number 6, the *Regional Health Information Organization (RHIO)*. Stakeholders represented: complex integrated hospital delivery system; community hospital; medical society officer; clinician; Massachusetts eHealth Collaborative EHR Project, physician group practice; Federal health agency; long-term care nursing home and hospice care; quality improvement organization; Commonwealth of Massachusetts, EOHHS.

2.5.2 Domains

MA-HISPC collected 41 business practices for this RHIO scenario. Barriers to HIE were indicated for 13 business practices involving domains number 9 Information Use and Disclosure with 6 BPs (46%), number 8 State Law Restrictions with 5 BPs (39%), and number 4 Information Transmission with 2 BPs 15%.

Domain and Business Practice Discussion

#9 Information Use and Disclosure

◊ Barrier

Technical: The RHIO and its providers must consider how much PHI really is needed to fulfill the intended purpose of a project. They should strive to use the minimum necessary under this scenario and use de-identified information whenever possible. A RHIO can collect de-identified data without patient consent or an IRB waiver of consent. In Massachusetts the transfer of identifiable patient data requires patient consent for any RHIO research (i.e. information that will be used to create new knowledge). On the other hand, if the information is not disclosed to third parties, and is used to create clinical benchmarks or for direct patient care (as part of an ongoing relationship), consent may not be needed, since this might be part of healthcare operations or patient care. In either event, a business associate relationship must be established and properly documented.

Legal: There are no Massachusetts law barriers to the use of medical information to monitor disease management if the data is de-identified and the patients are not contacted by the RHIO. Consent would be necessary for a RHIO to contact a patient for disease management purposes.

See the HIPAA legal comments within the technical discussion above.

◊ Business Practice

While anticipated, there currently is no business practice for this type of RHIO activity.

2.5.3 Critical Observations

For Solutions Working Group Considerations:

- The circumstances where a RHIO would be using identifiable data, including biosurveillance transmission to Department of Public Health, and clinical quality improvement information.

- Should there be different levels of de-identification, limited data set based on the potential of disease management activities? Disease management may need some definition; currently it is unclear. Participants should consider whether fully de-identified information can be used, whether de-identified statistical information can be created and used, or whether the participants can enter into data use agreements and use limited data sets.

- Provide more definition around use of a HIPAA limited data set to determine if it meets the HIPAA limited data set rules of use for research, public health, or health care operations.

2.6 Research (Scenario 7)

2.6.1 Stakeholders

The VWG interviewed ten (10) stakeholders representing seven (7) stakeholder types to collect the business practices and barriers for Scenario number 7, *Research Data*. Stakeholders represented: integrated hospital delivery system; complex hospital system; multi-site physician medical group practice; consumer, patient and parent; medical society officer; clinicians; Medical Center Institutional Review Board (IRB) staff, Federal health agency; the Commonwealth of Massachusetts EOHHS and Department of Mental Health.

2.6.2 Domains

MA-HISPC collected 33 business practices for this IRB scenario. Barriers to HIE were indicated for 12 business practices involving domain number 8 State Law Restrictions with 7 BPs (58%) and number 9 Information Use and Disclosure with 4 BPs (33%).

Domain and Business Practice Discussion

Domain Number 8 State Law Restrictions and Domain Number 9 Information Use and Disclosure

◊ Barrier

Legal: In this scenario the federal IRB requirements were coded as Domain Number 8 State Law Restriction barriers. Consent by a parent or guardian would clearly be required to extend an approved research period. Research is generally controlled by federal law (so-called Common Rule), and as a result, informed consent, which is the only Massachusetts legal barrier, must be obtained to permit the research to go forward. Use of existing research data to write a paper might require a new consent and authorization from the parent or guardian, but also could be permitted with a wavier from the IRB if appropriate subject protections were employed.

◊ Business Practice

Consent must be granted for any change in the research protocol unless an IRB waiver for minor (minimal) changes is obtained.

2.6.3 Critical Observations

For Solutions Working Group Consideration:

Currently, there is minimal interoperability around research studies in Massachusetts. Further, the issue of an additional written paper would have no impact on consumer as long as it de-identified any patients in the study. Of anecdotal interest, this scenario brings up a practical consumer consideration. If a parent or guardian was asked for additional consent to extend a pharmaceutical research project, the consent would be based on the value that has occurred for the patient in the study. Consumers indicated they would not be interested in additional time for the study if travel to appointments is time-consuming, and/or if the patient not responding well to the drug test. We did not identify any major state level barriers arising out of current practice; local researchers are used to working with the Federal Common Rule.

2.7 Law Enforcement (Scenario 8)

2.7.1 Stakeholders

The VWG interviewed two (2) stakeholders representing two (2) stakeholder types to collect the business practices and barriers for Scenario number 8, *Access by Law Enforcement*. Stakeholders represented: consumer advocate; and a consumer, patient, and parent.

2.7.2 Domains

MA-HISPC collected eight (8) business practices for this *Law Enforcement* scenario. Barriers to HIE were indicated for one (1) business practice involving domain number 9 Information Use and Disclosure with business practices (100%). In Massachusetts, the results of blood alcohol and drug screening tests are given to law enforcement agencies without patient consent, or per Massachusetts General Laws, chapter 90, section 24(e).

Domains and Business Practices Discussion

Domain Number 9 Information Use and Disclosure and Domain Number8 State Law Restrictions

◊ Barriers

Legal: A 19-year old is considered an adult under Massachusetts law and must provide consent for either law enforcement (absent legal process such as a court order) or parent access to PHI. The consent issues for law enforcement are half HIPAA, half Massachusetts law; and the age of majority is Massachusetts law.

◊ Business Practice

Emergency Room staff will ask the 19-year old if s/he wishes to share his/her PHI with his/her parents, if yes, the patient will sign a consent (authorization) form for PHI disclosure to the parents.

2.7.3 Critical Observations

For Solutions Working Group consideration:

- Will need to follow up with law enforcement stakeholder directly before the project determines that there are no issues. Law enforcement issues will be discussed and outlined in the legal, policy, communication and education parts of the Massachusetts implementation plan. We will suggest to the implementation project steering committee that a number of examples be developed that address both Massachusetts law and regulations and the HIPAA requirements for this scenario and other scenarios where law enforcement personnel normally interact. Emergency Departments indicate that during a patient's care, they provide very limited information to law enforcement.

2.8 Prescription Drug Use/Benefit (Scenarios 9 and 10)

2.8.1 Stakeholders

The VWG Project Team interviewed seven (7) Stakeholder types to collect information on business practices for Scenarios 9 and 10, *Pharmacy benefit management* and *PBM business development*. Stakeholders represented the following: multi-site physician medical group practice, Commonwealth of Massachusetts EOHHS and Department of Mental Health; clinician; Pharmacy Benefit Manager for regional health plan with mail order pharmacy division; consumer advocate, health plan payer; consumer as employee.

2.8.2 Domains

MA-HISPC collected 28 business practices for this *Prescription use/benefit scenario*. Barriers to HIE were indicated for eight (8) business practices involving domains number 4 Information Transmission Security with business practices (50%), number 2 Information Authorization and Access Controls with 2 (25%), and number 9 Information Use and Disclosure with two (2) business practices (25%).

There are no Massachusetts legal impacts in either of these scenarios for general medical information. Under Massachusetts law the patient has already signed for such information access when s/he signed up for medical insurance. The sensitive information impacts will be addressed during the implementation project.

Domain and Business Practice Discussion

Domain Number 4 Information Transmission and Security Exchange Protocols

◊ Barrier

Technical: All information from mail-order pharmacy to prescribing physician is by fax and in extreme circumstance by phone. Will not use e-mail without assurances of security.

Resource: Pharmacy Benefit Managers (PBMs) will not invest in secure e-mail transmissions until critical mass of physician usage is achieved.

◊ Business Practice

PBM or mail-order pharmacy contacts the prescribing physician to inform him/her that the prescription is not on the respective health plan formulary.

Domain Number 2 Information Authorization and Access Controls

◊ Barrier

Workflow: Most physicians have system set up to use a paper prior authorization form to fax back to PBM/mail-order pharmacy.

◊ Business Practice

Physician office receives PBM/mail-order pharmacy request for prior authorization information to justify the request to fill a prescription with a non formulary drug.

Domain Number 9 Information Use and Disclosure

◊ Barrier

Legal: HIPAA minimum necessary requirements.

Business Associate Agreement will need to be in place to share the PHI for sharing with a PBM. This would usually be between a health plan and the PBM. In most circumstances drugs provided by a mail-order pharmacy will need no Business Associate Agreement as the pharmacy is a HIPAA covered entity.

◊ Business Practice:

Physician has to provide additional PHI as to why formulary drugs may be inadequate.

2.8.3 Critical Observations

For Solutions Working Group Considerations:

- Real time access to formulary
- From a consumer advocate perspective, a patient is pleased to not be involved in the prior authorization process.

2.9 Healthcare Operations/Marketing (Scenarios 11 and 12*)*

2.9.1 Stakeholders

The VWG Project Team interviewed six (6) Stakeholder types to collect information on business practices for Scenarios 11 and 12, *Healthcare operations for an integrated delivery system*, i.e. an affiliated covered entity, and *healthcare operations for a single hospital entity*. Stakeholders

represented the following: complex integrated hospital delivery system; community hospital; physician group practice; clinician; Massachusetts eHealth Collaborative EHR Project; consumer as parent and patient.

2.9.2 Domains

MA-HISPC collected 26 business practices for these scenarios. Barriers to HIE were indicated for two (2) business practices involving domain number 9 Information Use and Disclosure with business practices (100%).

Domain and Business Practice Discussion

Domain Number 9 Information Use and Disclosure

◊ Barrier

Legal: HIPAA Privacy: need patient authorization for marketing

◊ Business Practice

Patient consent/permission required for the non-treatment, payment, and healthcare operations [HCO] processes. Marketing is not HCO.

LWG raised a question when discussing scenario 11: is this the sharing of PHI between two unrelated providers or are the hospital system and the tertiary an affiliated covered entity (ACE) under HIPAA?

- If the answer to the question is that the two providers are an ACE under HIPAA, there is no need for consent or authorization for the Six-Sigma team review / report or brochure.

- If the answer to the question is two unrelated providers, Massachusetts State law states that consent will be necessary.

2.9.3 Critical Observations

For Solutions Working Group consideration:

- No issues identified at this time.

2.10 Public Health/Bioterrorism (Scenario 13)

2.10.1 Stakeholders

The VWG Project Team interviewed four (4) Stakeholder types to collect information on business practices for Scenario 13, *Bioterrorism event*. Stakeholders represented the following: complex hospital system; clinician, medical society officer; Commonwealth's Department of Public Health state laboratory. All stated that there would be no barriers to the sharing of ePHI in a real bioterrorism event after the Governor declared such an event to be an emergency under the Massachusetts laws for civil defense and/or public health emergencies.

2.10.2 Domains

MA-HISPC collected 14 business practices for these scenarios. Barriers to HIE were indicated for two (2) business practices involving domain number 8 State Law Restrictions with business practices (100%).

Domain and Business Practice Discussion

Domain Number 8 State Law Restrictions

◊ Barrier

Legal: There is no specific Massachusetts law for a bioterrorism emergency. Massachusetts laws exist for civil defense emergency and for a public health emergency

While stakeholder interviews and the LWG uncovered state law and regulations for emergency situations, none of this addresses anything other than a civil defense emergency such as a weather emergency or lower grade public health emergency. The feeling was that current state law and regulations are insufficient for a bioterrorism event and would have to be stretched beyond typical or previous use to cover a true bioterrorism event in order to share data with law enforcement or media outlets. However, current state law is deemed sufficient for an event such as a flu pandemic.

On the other hand, state law and regulations that give the Department of Public Health permission to investigate, are sufficient authority to investigate anthrax exposure and other similar biological events.

It was also suggested that Massachusetts state criminal law might cover such a bioterrorism act as releasing anthrax.

Technical: Monitoring technology must exist in place before the event.

Cultural: Many clinicians do not know or understand the reporting requirements under Massachusetts law and regulations for suspected bioterrorism or potential epidemic situations.

2.10.3 Critical Observations

For Solutions Working Group considerations:

- Some major issues must be addressed in terms of remedial outreach, education and training programs to provide provider organizations, associations and trade organizations with opportunities to become more aware of requirements, procedures and legal reporting concerning suspected bioterrorism or potentially epidemic situations.

- The Massachusetts state law and regulations should be reviewed to ensure they are adequate to address events not previously experienced in the area of bioterrorism.

2.11 Employee Health (Scenario 14)

2.11.1 Stakeholders

The VWG Project Team interviewed two (2) Stakeholder types to collect information on business practices for Scenario 14, *Employee health information requests*. Stakeholders represented the following: Commonwealth's EOHHS and Department of Mental Health, consumer advocate.

2.11.2 Domains

MA-HISPC collected six (6) business practices for these scenarios. Barriers to HIE were indicated for four (4) business practices involving domains number 8 State Law Restrictions with two (2) business practices (50%), and number 9 Information Use and Disclosure with one(1) business practice (25%), and number 4 Information Transmission Security with one(1) business practice (25%).

Domain and Business Practice Discussion

Domain Number 8 State Law Restrictions

◊ Barrier

Legal: Under Massachusetts law there must be consent by the patient to share the medical information with the employer.

Technical: This is a verbal request/process. Stakeholders could not imagine this being a cut-and-paste from the medical record emailed to the employer

◊ Business Practice

Employee asks Emergency Department personnel to provide them with a return to work note. All providers have printed pads available for this use.

2.11.3 Critical Observations

For Solutions Working Group considerations:

- Secure transmission of specifically designed electronic form to employer
- Standard set of data elements

2.12 Public Health (Scenarios 15–17)

2.12.1 Stakeholders

The VWG Project Team interviewed eleven (11) Stakeholders, representing ten (10) types to collect information on business practices for Public Health Scenario 15, communicable *disease notification*, Scenario 16, *newborn screening*, and Scenario 17, *medical care for homeless shelter client*. Stakeholders represented the following: physician group practice; Commonwealth's newborn screening laboratory, Department of Public Health State Laboratory Institute, Department of Transitional Services; clinician; community hospital; integrated healthcare delivery system; community clinics and health centers; Massachusetts eHealth Collaborative EHR Project; homeless shelter.

The LWG had issues with scenario number16, newborn screening. It is not typical that the metabolic test results and diagnosis be sent to a specialty care center specializing in disorder care; nor would an Interactive Voice Response [IVR] system be used to share the metabolic test results and diagnosis.

2.12.2 Domains

MA-HISPC collected 71 business practices for these scenarios. Barriers to HIE were indicated for 23 business practices involving domains number 8 State Law Restrictions with nine (9) business practices (39%), and number 9 Information Use and Disclosure with eight (8) business practices (35%, and number 1 User and Entity Authentication with three (3) business practices (13%).

Domains and Business Practices Discussion

Domain Number 8 State Law Restrictions

◊ Barriers

Legal: For scenario 15 the Massachusetts Department of Public Health under its state law and regulations has the authority to contact the Department of Public Health in the other state to inform them of the name of the individual with Tuberculosis (TB). State public health authorities feel they have this authority in TB cases, but the law and regulations are less clear for other kinds of communicable diseases. Policy makers should consider creating more express authorization for sharing protected health information across state lines for public health purposes, especially in cases involving highly communicable diseases.

For scenario 17 all the transfers and/or sharing of medical information require consent under Massachusetts law.

For Scenario 17: State law requiring second consent for sensitive information is very cumbersome.

◊ Business Practice

Most notifications are by phone or U.S. mail. The state agencies are just beginning to use electronic means to share data specific to newborn metabolic testing as found in scenario 17.

While Massachusetts does most of the newborn screening for all New England states, state-to-state there is no uniformity in what tests are scheduled and performed.

In Massachusetts there is very little follow up after diagnosis by the state lab or other parts of the Department of Public Health.

Domain Number 9 Information Use and Disclosure

◊ Barrier

Privacy: Every time that a record is moved, minimum necessary is applied.

Technical: Newborn screen results are shared via US Mail to treating physician if the test results and diagnosis are normal, and by phone if abnormal. Lab is just beginning to use secure email.

For TB, such information across state lines is done today by phone, and it is anticipated that this will continue in the future given the risk of spread of infectious disease.

 # 1 User and entity authentication

◊ Barrier

Technical: Only paper consent (homeless shelter). Also, here must be a new consent at each step / movement of the patient's sensitive medical information.

2.12.3 Critical Observations

For Solutions Working Group Considerations:

- Scenario 15: It would be best if there were interstate agreements to share infectious disease information during an emergency (consider connection to Centers for Disease Control and Prevention or US Public Health Service). Goal is to get patient off the street as quickly as possible.

- Other states have tuberculosis laws, but are silent or differ on other types of communicable diseases; this is where cross-border sharing would be useful.

- It would be useful to know who to notify in the sister state, both the health authorities and the law enforcement authorities, and how to notify outside of business hours. It will also be important to know what types of communicable diseases can/should be committed to locked care facility.

- Scenario 16: Need to review the possibility of electronic notification to ordering physicians, and hospitals.

- Scenario 17: Homeless MIS initiative just being initiated, federal mandate through HUD, will be cultural change for shelters to communicate electronically beyond internal emails.

- Different stakeholders indicated range of PHI transmissions from paper to EHR, to fax and US Mail.

- Providers beginning to use EHRs would like a solution to second consent requirements since it represents a technical significant challenge to compliance

- According to some providers, specific consents for sensitive information create significant barriers from a technical point of view, simply because it is per instance consent requirement. Initial technical efforts to address the filtering of sensitive information within EHRs requires "filtering" logic to check against all available information in the record that may be transferred. From a consumer advocate point of view, sensitive health information consent requirements provide a high level of privacy protection for sensitive health information. LWG analysis suggests that more refined privacy protections that distinguish among

emergency disclosures, treatment disclosures, and other kinds of disclosures might be appropriate. Also, a more granular approach to documentation of consent in different kinds of circumstances might be appropriate for consideration.

2.13 State Government Oversight (Scenario 18)

2.13.1 Stakeholders

The VWG Project Team interviewed two (2) Stakeholder types to collect information on business practices for Scenario 18, *Health oversight, legal compliance/government accountability*. Stakeholders represented the following: medical school, Commonwealth's Department of Public Health.

2.13.2 Domains

MA-HISPC collected 12 business practices for these scenarios. Barriers to HIE were indicated for three (3) business practices involving domain number 9 Information Use and Disclosure with business practices (100%).

The LWG stated that scenario number18 would not likely happen in Massachusetts. Not all of the agencies asked to share data are covered entities, nor do they have other state authority to share such data. They could not decide if the scenario outlines a quality assurance issue or a healthcare operations use under HIPAA.

Domain and Business Practices Discussion

Domain Number 9 Information Use and Disclosure

◊ Barrier

Technical: Identifying target population would have to be a manual process, because provider does not keep income data on system

Privacy: Data would have to be de-identified which makes the purpose moot. The data exchanges outlined in this scenario would not happen in Massachusetts unless the information was completely de-identified.

Legal: There are a number of state laws and federal laws that complicate this scenario and all would need to be reviewed to determine if the data could be shared or needed to be shared as outlined in this scenario. First, from federal law, FERPA controls all school records and it has its own privacy and security concerns. Second, children in Massachusetts cannot register for and be accepted for kindergarten without having had the proper immunizations. Third, part of the Department of Public Health role is to compile and maintain the lead paint registry in the Commonwealth.

2.13.3 Critical Observations

For Solutions working group considerations:

- To accomplish this epidemiological project would require legislative mandate that would permit the creation of an appropriate data base without patient consent. Massachusetts law will be necessary to share this information.

- Technical and Resource: need data base requirements to be developed and funded.

2.14 Summary of Critical Observations and Key Issues

The stakeholder interviews and LWG analysis disclosed several recurring themes and issues:

- Stakeholders clearly identified state and federal laws protecting the confidentiality of "sensitive" categories of health information, such as AIDS/HIV, mental health, substance abuse treatment, and genetic testing, as creating challenges for electronic data exchange. No stakeholder identified a mature, well understood technical solution that facilitated the management of information exchange in strict compliance with these laws, especially in situations where sensitive data is intermingled with other medical data.

- Many stakeholders expressed the view that the "barriers" created by sensitive data laws are better thought of as appropriate privacy controls that fulfill socially desirable goals. The LWG discussed the possibility that some of these sensitive data laws might be refined to take into account different kinds of disclosures of information or different methods of collecting and documenting consent under differing circumstances (e.g., emergency care vs. payment).

- Stakeholder interviews disclosed uncertainty or differences regarding state law consent requirements for data exchanges relating to treatment, payment and healthcare operations. However, if the scenarios did not require the use of specially protected "sensitive" data, state law was not cited as a major barrier to interoperability.

- HIPAA requires that uses and disclosures of protected health information for anything other than treatment be subjected to "minimum necessary use" review, so that no more than the minimum necessary amount of information is used or disclosed in each situation. Many stakeholder interviews disclosed difficulty in fully understanding and applying "minimum necessary use" test. In contrast, some stakeholders indicated that the minimum necessary doctrine was in fact being applied in treatment situations.

- Numerous technical and infrastructure barriers to electronic interoperability were disclosed, e.g. the lack of interoperable secure email, especially for physician practices and small providers.

- Providers indicated a strong preference to pursue HIE interoperability initiatives that would "push" PHI from the holder rather than "pull." This distinction will be critical in a viable implementation plan.

- Financial resource limitations were frequently cited as a barrier to interoperable data exchange. Similarly providers indicated that while their investments in data exchange technology might create return on investment for payers, government agencies or others, it was unlikely to generate sufficient financial return for providers to justify large investments.

- Many providers expressed a high level of comfort with existing business practices for data exchange (e.g. telephone consultation followed by faxed documents) and expressed doubt that a more automated process would present substantial advantages.

- Public health authorities noted that interstate communication of identifiable health information is not explicitly addressed in many state laws, and that more explicit authority for interstate cooperation to facilitate treatment and public health goals would be desirable.

The RTI review of the MA-HISPC interim variations report stated that "no e-HIE 'good practices' were identified." This is correct. The MA-HISPC SWG and IPWG phases began to identify good e-HIE practices.

- Of important note is the addition of the best practice to "push" clinical information rather than allow it to be pulled.

- Best practices were identified during the MedsInfo ED project where the need for patient consent was not confirmed as required, but the business practice implemented informed consent and requested that each patient agree to proceed with an internet software application search for medication history. Further, considerable specifications were developed with stakeholder consensus for required audit elements and live report capability.

Best practices continue to come to the attention of the MA-HISPC Project Team as we have the opportunity to share the project experiences with stakeholder groups. The MAeHC projects are at the point in their implementation where best practices with respect to opt in are being documented and shared.

Please note that the interim variations report focused on the barriers, and the remaining practices were essentially best practices. Further, HIE best practices are still in the paper world. eHIE best practices are just emerging.

3.0 Summary of Key Findings from the Assessment of Variation

3.1 Description of the main findings from the interim assessment of variations report, prioritize key findings (top 5 to 10 identified privacy and security issues), and the rationale for prioritization.

The stakeholder interviews and Legal Working Group (LWG) analysis disclosed several recurring themes and issues:

- Clearly identified state and federal laws protecting the confidentiality of "sensitive" categories of health information, such as AIDS/HIV, mental health, substance abuse treatment, and genetic testing, as creating challenges for electronic data exchange.

  No stakeholder identified a mature, well understood technical solution that facilitated the management of information exchange in strict compliance with these laws, especially in situations where sensitive data is intermingled with other medical data.

- Expressed the view that "barriers" created by sensitive data laws are better thought of as appropriate privacy controls that fulfill socially desirable goals.
    - The LWG discussed the possibility that some of these sensitive data laws might be refined to take into account different kinds of disclosures of information or different methods of collecting and documenting consent under differing circumstances (e.g. emergency care vs payment).

- Disclosed uncertainty or differences regarding state law consent requirements for data exchanges relating to treatment, payment, and healthcare operations. However, if the scenarios did not require the use of specially protected "sensitive" data, state law was not cited as a major barrier to interoperability.

- HIPAA requires that uses and disclosures of protected health information for anything other than treatment be subjected to "minimum necessary use" review, so that no more than the minimum necessary amount of information is used or disclosed in each situation.
    - Many interviews disclosed difficulty in fully understanding and applying "minimum necessary use" test. Further, some stakeholders indicated that the minimum necessary doctrine was in fact being applied in treatment situations.

- Numerous technical and infrastructure barriers to electronic interoperability were disclosed, e.g. the lack of interoperable secure email, especially for physician practices and small providers.

- Financial resource limitations were frequently cited as a barrier to interoperable data exchange.
    - Similarly, providers indicated that although their investments in data exchange technology might create return on investment for payers, government agencies or others, it was unlikely to generate sufficient financial return for providers to justify large investments.

- Many providers expressed a high level of comfort with existing business practices for data exchange (e.g. telephone consultation followed by faxed documents) and expressed doubt that a more automated process would present substantial advantages.

- Public health authorities noted that interstate communication of identifiable health information is not explicitly addressed in many state laws, and that more explicit authority is needed for interstate cooperation to facilitate treatment and particularly in urgent situations for public health purposes (e.g., a large accident near a border or a communicable disease incident).

3.2 Description of 'effective' practices identified by the state, including overall practices that protect privacy and security and permit or advance interoperable electronic health information exchange (and that cut across multiple domains specified in the contract) as well as practices identified within each of the nine domains (a brief description of the definition of 'effective' practice should be provided)

There are several Massachusetts practices that have been identified as effective.[2] Effective, in this context, is defined as a practice that meets the current HIE requirements without hindering the workflow or healthcare quality delivered to the patient.

- Treatment Scenarios: Business practices regarding initial consent and second consent associated with the transfer of sensitive information (as legally defined) are effective in protecting PHI while providing high quality care regardless of the type of process (paper or electronic). Many processes remain non-electronic, e.g. phone and fax, with clinicians reporting that the richness of clinical information being exchanged is superior to a structured data exchange that could lose the nuances of a telephone exchange. Domains including 8, 9, 1, 4, 2, 7, 5, and 3 were associated with these practices.

- Payment Scenario: Currently, health plan case management activities to approve inpatient hospital stays take place in the facility and as such, the case managers are authenticated by the facility to gain access to clinical information. This process is thought to be effective because the case managers go through the same authentication processes as do other clinicians. Domains including 9, 4, and 8 were associated with these practices.

- RHIO Scenario: The RHIO can collect de-identified data without patient consent. If PHI is needed for the project, the minimum necessary restrictions will be applied. The current process provides protection of PHI while affording the RHIO a way to use the data for population-based, care management studies. The mechanics of collecting data are complex and must be understood. Domains including 9, 8, and 4 were associated with these practices.

- Research Scenario: Research projects generally use the facility's IRB to gain access to clinical information. Patient consent is gained at the start of the patient research part of the process. Patient consent is typically not obtained for subsequent data research and analyses. Any changes in protocol or use of outcome information need to be approved (or waived) by the IRB. Domains including 8 and 9 were associated with these practices.

- Law Enforcement Scenario: In Massachusetts, a person is considered a legal adult if they are 18 or older. As such, they will be under the rules governing patient consent and asked before their PHI is released. Only Massachusetts law or court order would allow release without patient consent. Domain 9 was associated with these practices.

- Prescription Drug Use/Benefit Scenarios: Currently, practices are fax or phone. This is considered effective by the PBM and they are not likely to change their practices without a preponderance of secure email transmissions by clinicians. Domains including 4, 2, and 9 were associated with these practices.

[2] The summaries below reflect the data that we heard during our interviews with stakeholders. Not all members of the SWG agree with the perspectives of the interviewed stakeholders.

- Healthcare Operations/Marketing Scenarios: The business practices are not likely to be affected by the availability of HIE. Patient consent is needed to use clinical data for marketing purposes. Domain 9 was associated with these practices.

- Public Health/Bioterrorism Scenarios: The authorization of the use of PHI would come from the Governor during a healthcare crisis. Domain 8 was associated with these practices.

- Employee Health Scenario: Currently, this is not an electronic process but rather, a voice request and manual one. Domains including 8, 9, and 4 were associated with these practices.

- Public Health Scenarios: In Massachusetts, metabolic test results and diagnoses would not typically be sent to a specialty care center nor would an Interactive Voice Response (IVR) system be used to share the metabolic test results and diagnosis. In the scenario involving TB, Massachusetts public health authorities have the authority to name the individual, but the law and regulations are less clear for other kinds of communicable diseases. Domains including 8, 9, and 1 were associated with these practices.

- State Government Oversight Scenario: The MA-HISPC Legal Working Group (LWG) stated that this scenario would not likely happen in Massachusetts because not all the agencies asked to share data are covered entities, nor do they have other state authority to share such data. Domain 9 was associated with these practices.

MA-HISPC identified eight (8) barriers to HIE[3]:

- Technical: The inability to electronically transfer data-references the lack or current shortcoming in format compatibility, semantic interoperability, transmission interoperability

- Legal: Existing Federal, Massachusetts law and regulations governing use and disclosure of health information

- Cultural: Healthcare staff at covered entities indicated that current procedures to information exchange work are sufficiently timely, and provide accurate data exchange. Thus the need to change is not compelling. In addition, to a significant degree, the consumer role has not been part of the process to date.

- Privacy: Some privacy rules, such as the need for consent (under Massachusetts law), HIPAA authorization, the application of the minimum necessary, and other HIPAA requirements are identified as barriers. In other cases, providers may decline to disclose information even when allowed by applicable privacy rules because of concerns that the downstream recipient will not protect the patient's privacy. Some privacy barriers may be viewed as appropriate, even if they are strong barriers to interoperability.

[3] The term "barrier" is used based on the Report guidance requests. MA HISPC would like to note that our stakeholders believe this term to have negative connotations: some barriers serve important roles in protecting privacy and security safeguards and maintaining appropriate controls; the good barriers were outlined in the MA HISPC Interim Variation Report.

- Workflow: With training, education and better capabilities, electronic HIE could occur. (Not only training – but physical re-arrangement of environments.)

- Perception: Many in the healthcare workforce follow a procedure believing it is driven by a legal requirement; both Massachusetts state law and HIPAA. These perceptions are not necessarily accurate.

- Security: The current architecture of the technical application does ensure appropriate access controls, authentication, and role-based capabilities. The current manual systems for access control and authentication rely on routine nature of requests and trust factors between individuals and entities.

- Resources: A covered entity/organization does not have either the personnel or the funds to allocate to electronic HIE initiatives.

3.3 Identification of variations identified by the state and NOT being addressed by the proposed solutions presented in this report

Changes in HIPAA regulations and state law restrictions are not generally addressed by the proposed solutions presented in this report. Solutions involving education, policy development, and technology are discussed in detail.

4.0 Introduction to Analysis of Solutions

The solutions described in the Interim Solutions Report represent a synthesis of the full breadth of SWG stakeholder discussions regarding how to move to Massachusetts' public and private interoperability HIE goals and initiatives forward. Considerations as to solutions' feasibility and priority were included in all discussions, and formed the basis and framework for Deliverable #4, the Interim Implementation Plan. Importantly, SWG stakeholders identified the following important underlying observations:

- Unmet resource needs, both the actual dollars required for providers and plans to purchase required technology, and the group process/in kind contributions that have been made to date to move HIE forward; but this source of support cannot be expected to continue.
- Determining a satisfactory level of consumer and patient input. MA-HISPC has included such stakeholder input throughout the project, and has plans to address additional advocacy groups; the question remains, however, "Is this adequate?"
- Recognizing the need to address data ownership issues as HIE moves forward. Implementation must include provisions for the rights to and accountability for clinical data.

MA-HISPC has four (4) broad overarching observations that have been developed from the MA-HISPC solutions work.

- There must be intense engagement with the consumers of medical care (the patients) in all enterprise wide and statewide HIE and interoperable solutions work and implementation. Consumers are often the last group to be included for input when procedural changes are planned. If consumers are going to support, invest in, and use the changes that HIE and interoperability bring, they must be engaged at each stage of planning and implementation.

- An implementation project, no matter how well designed, will not move forward without sufficient funding and extensive knowledgeable resources. An earlier HIE pilot initiative in Massachusetts was accomplished at a value of $1.3 M; half of those dollars were in-kind contributions and in-kind investments. A current EMR and HIE project in Massachusetts is staffed by 20 employees, with additional donated provider/practice resources, and numerous consultants. Indeed it is estimated that it would take $400 million to expand this project statewide. Volunteer work will not be sufficient and cannot be sustained as the solution to accomplish viable HIE interoperability in any state or territory.

- Massachusetts recognizes the need to address data ownership and use issues. State law and regulations are not well understood across the industry. Of note is the probability that the improved efficiency from technology changes will complicate ownership and use issues. The issue of data "ownership" and use must be addressed directly as part of any implementation plan as well as included in both policy and education solutions.

- The Massachusetts healthcare stakeholder community has demonstrated success at consensus building over 30 years as a result of the neutral convening provided by the MHDC. There is a need to expand this work in building enterprise wide and statewide HIE and interoperability best practices and policies. MA-HISPC has learned in the data collection and VWG and SWG meetings that the previous and ongoing HIE and interoperability projects have created a substantial baseline from which to proceed. The Massachusetts implementation project will include collection of this baseline data, and policies and procedures, and consensus building.

5.0 Review of Massachusetts Solution Identification and Selection Process

5.1 Overall process used by Massachusetts HISPC to develop solutions

Between November 7, 2006 and January 4, 2007, MA-HISPC Project Team convened the SWG, and developed an approach for the identification of solutions to interoperability in an iterative manner. The challenge was to establish and document a process that would review the eight (8) categories of barriers and the thirty (30) critical observations identified from the variations in business practices activities to determine the best method to focus the activities of the SWG. The Project Team employed some trial and error to determine the most useful presentation of synthesized collected and analyzed data that would prove most useful and comprehensive for SWG solution identification and implication discussion. In all, four (4) approach iterations were developed and "tried," including framing by scenario, barrier, issue or recommended solution. In addition, to support a viable approach, the Project Team has taken advantage of relationships established at the HISPC Regional meetings and has participated in the RTI sponsored WebEx presentations that have assisted in providing guidance for a valuable Deliverable.

During the SWG work, the data collected by the VWG and the LWG were reviewed, nuances added, and issues refined. The Project Team held follow up individual and group meetings to collect additional data that was discovered incomplete or missing in the SWG process. The MA-HISPC project phases have all dovetailed nicely in that each phase permitted the original data collected to be added to and re-sorted. Each phase has informed the next phase very well and Massachusetts has developed a very strong foundation.

5.2 MA-HISPC Solutions Workgroup

The Solutions Workgroup was comprised of 17 stakeholders. Each was selected based on several factors: participation during the variations of business practices activities; participation on the Steering Committee; and current legal, compliance, operational, policy, or clinical experience with HIE activities in Massachusetts or nationally. The SWG is charged with developing a process to review and consider current barriers to HIE interoperability within a context that identifies stakeholder issues and challenges and then translates these considerations to potentially viable solutions. The following stakeholder groups are represented on the SWG:

- Commonwealth of Massachusetts – legal counsel
- Commonwealth of Massachusetts – security officer and technical architect
- Two Private Practice attorneys – national privacy and security reputation
- E-Health Consumer Advocate
- MHDC CEO and attorney
- Psychiatrist and President of Massachusetts Psychiatric Association
- Clinician and Complex Hospital System Corporate Compliance
- Complex Hospital System, Corporate Director, Health Information Services
- Complex Hospital System, Corporate Manager, Confidentiality
- Chairman, HITSP
- Community Hospital CIO, VP IT
- Project Manager, Clinic Research Department, Privacy and Security Officer Safe Health
- Health Plan Security Officer
- Executive, Statewide EMR Pilot Project
- Community Health Centers, Director Technical Services
- Mental Health and Substance Abuse Association, Project Manager

5.3 Process used by MA-HISPC to identify and propose solutions

The SWG Stakeholder convened five (5) times between November 16, 2006 and January 4, 2007. Results of SWG activities were reviewed by the Steering Committee in December and January. The solution identification process began with a review of the 30 critical observations described within the context of the 18 scenarios in the Variations Report. It became apparent that the information collected would be more usefully discussed if it were organized by issue within barrier category. The data were re-sorted several ways before arriving at an approach that allowed a full scope of discussion while providing a structure to capture the needs, issues and translation of these to solutions. The stepwise process included: a SWG Issues and Challenges spreadsheet categorized by Barriers (cultural, technical, workflow, legal, resource, perception, security and privacy), and included domains affected; SWG discussions expanded to 95 needs and issues that included domains and referenced the original scenarios. From these, a final multi-dimensional spreadsheet was developed that captures and translates the overlap of 9 issues that could be resolved by one or all of four categories of solutions. The nine issues to be resolved are: consent; minimum necessary; sensitive information; secure communication; audit; access; common standards – definitions – templates; RHIOs; and risks and benefits of HIE. The high-level solution categories are: legal, technical, policy or educational.

5.4 Process used by the MA-HISPC to vet, evaluate and prioritize solutions

The Solutions Work Group represents a formidable number of current HIE stakeholders as they continue to consider the implications of the full scope of recommendations. Evaluation of feasibility and prioritization has been included in all SWG meeting discussions. The value of a scoring system has been discussed and is being explored. Additionally, at its last meeting, SWG participants agreed that they would continue to represent the Project as participants on the Implementation Plan Work Group, thereby bringing a very high level of continuity to the Project. Further, once the Solutions Report is complete, the Steering Committee has asked the Project Staff to prepare a one-page summary of the process and distribute it to stakeholder wider constituencies for additional comment. In addition, the MA-HISPC Project Manager presented to the Project activities to consumer and privacy stakeholders through collaboration with a consumer advocacy organization, Health Care For All.

5.5 Solutions – Organization and Presentation

MA-HISPC's Project Team has approached the presentation of solution information in Section 4 in a manner that accommodates its four solutions categories (legal, technical, policy and education) by addressing each of these with a definition and then a discussion of the most significant issues of patient consent, sensitive information, access controls, and community standards. To be responsive to the RTI outline request for several different "cuts" at the information, MA-HISPC first discusses its solutions framework under a Section labeled III b. The report then returns to the RTI outline and answers the other nine questions, labeled: a,c,d,e,f,g,h,i, and j per proposed solutions.

5.6 Description on how Massachusetts has determined the level of feasibility of identified solutions

The MA-HISPC Project has, to date, discussed the level of feasibility of identified solutions based on its collective experience with HIE, that recognizes the broad implications of new initiatives, initial support, implementation challenges, lessons learned both broad and individual, and the underlying challenges of resources, potential consumer issues, and long term integration projects and goals.

6.0 Analysis of Massachusetts Proposed Solutions

6.1 Solutions to variations in organization business practices and policies

6.1.1 Governance-related solutions

MA-HISPC does not feel that the Massachusetts healthcare community has governance-related issues requiring solution since collaborative healthcare provider and payer roles have been in place, are workable, and have been refined for over 20 years. Further, MHDC has been convening stakeholders for almost 30 years.

MA-HISPC laws and regulations solutions are recorded in the legal solution section of the Interim Analysis of Solutions Report.

MA-HISPC identified a number of legal issues relating to HIE and corresponding legal solutions. These solutions are responsive to barriers and issues identified by stakeholder interviews and the Legal Working Group.

Patient Consent

The healthcare community must understand and implement technically supportable consent management. Consent management requires:

- Understanding of the state laws and regulations and the ability for users to have access to the state laws and regulations when necessary,
- Technical specifications that document the architecture and the patient and provider user requirements and directives for HIE,
- Baseline business and technical policies, and
- Continuing education and training for providers, payers and consumers regarding state and federal laws in order to assist in dispelling myths, and dealing with cultural and perception issues.

These four areas will be described in greater depth in the legal, technical, policy, and educations solutions within this part of the MA-HISPC Analysis of Solutions Report.

The Commonwealth has long had patient consent laws and regulations for the use and sharing of general medical records, and a legal definition of what is considered sensitive clinical information under state laws and regulations. The patient consent state laws and regulations have a great influence on HIE, whether in the form of paper work flows or electronic records and data exchange. However, not all stakeholders understand the legal definitions nor do they limit their concept of sensitive information to those definitions.

The MA-HISPC's Project Team anticipates that implementation planning, Deliverable #4, will include an outline of steps for a comprehensive review of the state's laws and regulations that speak to patient consent for the use and disclosure of clinical records. An additional solution within this category is the following recommendation: that the output of the comprehensive review of laws and regulations that apply to consent be available and accessible to the widest scope of stakeholders.

The MA-HISPC Project representatives will monitor for specific refinements in the state's patient consent laws and regulations since these may be proposed by the legislature or outside organizations and individuals, especially to authorize HIE for treatment, payment and health care operations.

The stakeholders convened for the MA-HISPC project may also work with The National Conference of Commissioners on Uniform State Laws (NCCUSL) to work on a uniform consent form.

Sensitive Medical Information:[4]

The healthcare community must understand and address the need for improved management of sensitive information. The goal is to establish a clear understanding of what is sensitive medical information, so that we can develop a process across the stakeholder community which can support appropriate and trusted use of the information, including appropriate privacy and security controls. This will consist of four major areas;

- Understanding the state laws and regulations and the ability to have access to the state laws and regulations when necessary,
- The technical needs for sensitive information management within an EHR and RHIO
- The baseline business and technical policies that need to be in place for sensitive information management, and
- Current and continuing education on state laws and regulations and federal laws to assist in dispelling myths, in dealing with cultural issues, and the different perceptions between and among the provider and payer communities and how it differs from consumer perceptions.

These four areas will be described in greater depth in the legal, technical, policy, and educations solutions within this part of the MA-HISPC Analysis of Solutions Report.

There are no known imminent legislative changes in the state law and regulations dealing with sensitive information that include mental health information, HIV-AIDs information, genetic information, sexually transmitted diseases, sexual assault and abortion for minors. Across the healthcare community these laws and regulations are seen as positive privacy protections.

The legal solution implementation plans will also discuss the federal Substance Abuse law and regulations, since this law has serious impact on consent management planning and implementation.

As part of the Implementation Planning, Deliverable #4, the MA-HISPC Project anticipates a process that will consider a comprehensive review of the state's laws and regulations that speak to sensitive information for the use and disclosure of clinical records that contain sensitive information. The Implementation Plan will outline steps for any comprehensive review to include varying interpretations of state laws and regulations that apply to sensitive information. It will outline implementation steps and structure stakeholders for consensus building and balance with recognition that some areas are unclear..

An additional solution within this category may be the recommendation that the output of such a comprehensive review of laws and regulations that apply to consent will be understandable and made available and accessible to the widest array of stakeholders possible through the use of multiple modalities.

[4] Both stakeholders and the Legal Working Group used the term "Sensitive Health Information" as a general term for categories of PHI that are entitled to additional legal protection beyond that specified by the HIPAA privacy rule. This is generally understood to include HIV-AIDs test results, substance abuse treatment information, mental health information (including records of psychiatrists, psychologists, social workers, and other therapists), mammography information, abortion for minors, sexual abuse counseling, and genetic test results. Some stakeholders suggest that other categories should be added by consensus or by patient preference.

Access Controls

Access controls are required by the requirements under the HIPAA Security regulation. This is not addressed by any Massachusetts state law or regulation. State departments and agencies must keep the mandates and requirements within the Commonwealth of Massachusetts's Fair Information Practices Act (FIPA).

The MA-HISPC Project has determined that the HIPAA Security regulation requirements, especially those bearing on access controls and role authorization, are not well understood, and may need further explanation to the provider and lay/consumer communities. Ongoing education will be necessary as the use of electronic transactions increases, to enable providers to understand the requirements of the HIPAA security rule.

The Implementation Plan will outline any need for HIPAA Security regulation requirements explanation and education. It will outline implementation steps for stakeholder consensus building. Any explanatory documents will be widely available and accessible to the healthcare community and other stakeholders.

The RTI review of the MA-HISPC interim analysis of solutions stated that the access control area is not detailed enough. S/he went on to suggest that authentication also be addressed in the final report. MA-HISPC recognizes that access controls and authentication are very important, as are the other security controls suggested in the first seven domains. All security domains are to be part of any implementation project.

Many of the RTI reviewer comments for both the variations and solutions documenting the issues and suggestions will be addressed in the April 16th Deliverable.

Community Standards

The stakeholders convened for MA-HISPC agree that a major impediment to working on community standards is lack of common understanding of both state laws and regulations, and federal regulations around the privacy requirements and the mandate to protect medical records and clinical information. Within the provider, consumer, and patient communities there are different understandings of both state laws and federal HIPAA regulations. Stakeholders agree that proper use of electronic signatures under state and federal laws and regulations need to be reviewed and outlined, so that providers, payers and others can implement electronic signature systems that comply with both federal and state law in a consistent and interoperable manner.

The MA-HISPC Project anticipates conducting a comprehensive review and interpretation of both state laws and regulations, and federal regulations concerning the privacy requirements and mandate to protect medical records and clinical information, including consensus building and the recommendation that any output be available and accessible to the widest scope of stakeholders and public usage.

6.1.2 Business arrangement solutions

The MA-HISPC business arrangement solutions have been previously discussed because health information electronic data exchange in Massachusetts is in varying stages of development. In the private sector, significant attention has been focused on HIE projects that move interoperability forward through pilot initiatives. These pilot projects have provided significant lessons learned on organizational,

contractual, policy and relationship building blocks for future HIE. Other private sector HIE projects have been designed for immediate business sustainability, ongoing growth, and scalability.

Other MA-HISPC business arrangement solutions are recorded in the policy solution sections of this Final Analysis of Solutions Report.

The MA-HISPC Policy Solutions are intended to help stakeholders engage in HIE while complying with legal requirements, meeting consumer expectations, and improving patient care. The policy solutions are intended to develop and promulgate consensus polices for use within the stakeholder communities. Polices should not only facilitate HIE, but should also reflect community consensus that some "barriers" to HIE are appropriate privacy and security controls.

Patient Consent

Policy solutions are the next step after understanding the Massachusetts laws and regulations regarding patient consent, permission, and/or authorization. This is seen as a three-pronged approach:

- Policy forums may be held with healthcare community stakeholders, including stakeholders to educate, train, and collect information concerning opt-in process for HIE or RHIO data sharing.
- Policies and procedures may be drafted addressing patient consent and sharing patient consent.
- These developed policies and procedures with stakeholder consensus may be implemented across the HIE enterprise, including policies to enable consent at one point of care to flow down to all clinicians and clinical points of care

The patient consent and sharing patient consent policies and procedures developed, may be posted on stakeholder community member websites for review and download.

Sensitive Medical Information

The MA-HISPC Project may develop and disseminate a uniform definition, or set of definitions, of the categories of sensitive clinical information based on state laws and regulations.

A process to identify and classify the sensitive information within EHR databases could be developed, and rules created for sensitive data use and sharing as part of implementation planning. Similarly, policies may be developed for sharing medical records and clinical information with law enforcement in the area of communicable diseases, and bioterrorism events. This is not an expansion of law enforcement access to protected health information, but only the development of policies to implement existing laws, and would be confined to handling extraordinary events.

The consumer community may be consulted in order to better understand and compare their definition of sensitive clinical data and how it compares with state laws and regulations

To the extent possible, all documents and outlines anticipated within this solution should be made accessible and available to the healthcare community through website initiatives.

Access Controls

The MA-HISPC Project has stated that community-wide policies and procedures are needed for appropriate access to shared and non-shared clinical information with an HIE system.

During the MA-HISPC implementation planning, the steps to draft, review and implement policy and procedures for access to shared and non-shared clinical information within an HIE system may be outlined.

To the extent possible, all documents and outlines anticipated within this solution should be made accessible and available to the healthcare community through more global website initiatives.

Community Standards

Solutions that address community standards solutions will require that policy be developed first, before technical solutions and then any education solutions can be developed. Technical and education solutions should reflect both legal requirements and policy preferences of the communities served. The stakeholder community may hold a series of forums to discuss, outline, and develop standards for all six HISPC project security domains,

- User and entity authentication
- Information authorization and access control
- Patient and provider identification
- Secure information transmission
- Information protection
- Information audit

The stakeholder community may also hold sessions to draft community standards for consent management and sensitive information management.

The agreed upon community security standards and consent management and sensitive information management standards may be published on a stakeholder community member's website for review and download.

6.1.3 Technical solutions

MA-HISPC technical solutions are recorded in the technical solution section of the Interim Analysis of Solutions Report. We would note that Massachusetts has already implemented pilot technical solutions specific to HIE, such as a record locator service that may not be available in other areas of the country.

The MA-HISPC stakeholders feel strongly that better solutions for technology challenges are required to facilitate HIE. In particular, better solutions are needed to address each of the four main issues already identified by the stakeholder interview process: consent management, sensitive health information, access controls and the implementation of community-wide standards.

Patient Consent

Once the legal and policy steps are completed, the healthcare community should work on outlining a streamlined process for the technical requirements to capture, share and implement patient consent management. The stakeholders convened to work on the MA-HISPC project may work together to design and implement a statewide consent form for general medical records, and for the use and sharing of sensitive clinical information. The SWG sees a model consent form as useful in both paper and electronic work flow systems.

The SWG recognizes that a patient's consent preferences may change over time, especially after changes in health status. However, the MA-HISPC stakeholders recognize that technology does not yet permit enterprise wide sharing of patient consent in a manner that will easily accommodate changes in the patient's medical condition and similar parameters.

Despite the current technical restrictions, the stakeholders identified the need to implement electronic systems in the future that will:

- Capture and share patient opt-in and other preferences
- Capture and record state laws and regulations consent triggers
- Flag sensitive data (internal to the application)
- Flag sensitive data in a specific patient's electronic records (internal to the application)
- Block external access to internally "flagged" sensitive data actions (implement blocking in such a way that does not inadvertently disclose the existence of, or type of, sensitive health information that was not transmitted), coupled with effective communication to system users that some kinds of information may be blocked; in this way, clinicians can use the system appropriately with patients
- Capture patient consent at one point in the system and flow this information to all clinicians and clinical points of care
- Be able to record and implement changes in consent with changes in patient's medical and clinical conditions

The Implementation Plan will outline the process for consent management. It is the intent of the project that all documents and outlines anticipated within this solution will be accessible and available to healthcare community for all to review and if possible download.

Sensitive Medical Information:

Once the legal and policy steps are completed the stakeholders convened for the MA-HISPC Project may work together to: outline the technical requirements for second consent and the use and sharing of sensitive information; and to design and implement one statewide consent form for both general medical records and the use and sharing of sensitive clinical information. This consent management is outlined as part of the technical solution, since any standard statewide consent form must be used in both a paper work flow and an electronic system. Further, MA-HISPC stakeholders recognize that technology does not yet permit enterprise wide sharing of patient consent for sensitive information at a granularity which would accommodate a change in medical condition and other such variables and parameters.

Despite the current technical restrictions, project stakeholders recommend that electronic systems in the future be implemented to enable:

- Identification and classification of sensitive information within databases
- Sensitivity flags be created for use in the EHRs and RHIOs
- Data filtering technologies to filter sensitive information based on state laws and regulations
- Create second consent technical procedures; create alerts with definitions informed by CPT and ICD 9, or IDC10, codes and other indicators

MA-HISPC's implementation planning will include stakeholders' input to outline the process for sensitive information management. The MHDC's experience with filtering sensitive drug history information as part of the MedsInfo-ED project suggests that development and implementation of filtering systems requires significant resources.

To the extent possible, all documents and outlines anticipated with this solution should be made accessible and available to the healthcare community through various methods including website initiatives.

Access Controls

A first step in the access controls area may involve the determination of a uniform standard for roles/ rules/definitions for access within a covered entity; and limited purposed access by outside organizations. Access controls must anticipate different rules to account for access by medical staff, health plan staff, and the consumer-patients and their proxies. Other access controls are needed within an EHR for data exchange between provider and community systems as well as for patient/consumer portal access to facilities' EHR.

During the MA-HISPC's implementation planning, a process will be outlined for determining a uniform standard for roles/rules/definitions for access within a covered entity; and limited purposed access by outside organizations. This may include rules-based access to sensitive clinical information.

To the extent possible, all the documents and outlines anticipated within this solution should be made accessible and available to the healthcare community through website initiatives.

Community Standards

The MA-HISPC stakeholders concur that it is important to begin outlining and reaching consensus on statewide technical standards and solutions. They emphasized the criticality of version control standards, policies and procedures, and the need to include these during early work on community standards to build trust in health information exchange.

MA-HISPC's implementation planning will include process steps to reach this agreed upon statewide technical standards and solutions. Areas that may be included in the discussion are consent management, sensitive information management, access controls and other security controls such as user and entity authentication, information authorization, patient and provider identification, version controls, information protection, information transmission protocols, audit, and administrative and physical safeguards. In addition, the implementation plan will outline tasks to develop a detailed set of requirements and specifications to be shared with vendors.

To the extent possible, all the documents and outlines anticipated within this solution should be made accessible and available to the healthcare community through website initiatives. Our intention is that this information be useful to standard setting organizations and to those engaged in the process of harmonizing technical standards.

6.1.4 Guidance/Education solutions that address misinterpretation issues

MA-HISPC guidance and education solution(s) are recorded in the education solution section of the Interim Analysis of Solutions Report.

MA-HISPC feels strongly that more and better education solutions must be developed for all stakeholders, including consumers, payers and government officials. Education solutions are important

for every issue identified in this report. Education solutions cover a wide range of activities from public awareness to professional continuing education.

Patient Consent

The MA-HISPC Project agrees that an education package based on the laws and regulations that deal with patient consent should be developed to help dispel cultural and perception barriers, as summarized in Section 2 of this report. Target audiences for improved understanding should include consumer, provider, and all the stakeholder communities.

MA-HISPC's implementation planning may outline educational steps to develop and share any approved patient consent form and patient consent policies and procedures with the greater consumer and provider communities.

A number of outreach and communication efforts need to be investigated, including:
- Face-to-face training
- Community forums
- Teleconference
- Webex conferences
- Newsletters
- Web posted news and alerts
- Brochures
- Mass media

The education package for use within provider facilities and physician offices may be posted on a stakeholder community member's website for use and download.

Sensitive Medical Information

MA-HISPC Project determines that an education and training package based on the laws and regulations, policies and procedures, and technical controls related to sensitive information management may fulfill an unmet need across the stakeholder communities. The Implementation Plan may address the needs to create an educational package.

A number of outreach and communication efforts may be investigated, including:
- Face-to-face training
- Community forums
- Teleconference
- Webex conferences
- Newsletters
- Web posted news and alerts
- Brochures
- Mass media

The education package may be posted on a stakeholder community member's website for use and download—at minimum information will be available and accessible.

Access Controls

MA-HISPC stakeholders agree that an education package based on the legal requirements, the technical standards and the policies and procedures for access control and all other security polices and procedures developed in the community standards work under any and all MA-HISPC proposed solutions. The Implementation Plan may outline the steps to create such an educational program for the consumer, provider, and stakeholder communities, and will describe the legal requirements, the technical standards and the policies and procedures for access control and all other security polices and procedures developed in the community standards work under any and all MA-HISPC's proposed solutions.

A number of outreach and communication efforts need to be investigated, including:
- Face-to-face training
- Community forums
- Teleconference
- Webex conferences
- Newsletters
- Web posted news and alerts
- Brochures
- Mass media

The education package may be posted on a stakeholder community member's website for use and download —at minimum information will be available and accessible.

Community Standards

MA-HISPC stakeholders agree that an education strategy based on the HIPAA privacy mandates and the state privacy law and regulations would provide significant value to the healthcare community. The Implementation Plan may outline the steps to create an education program to share with the consumer, provider, and all the stakeholder communities, outlining and explaining HIPAA privacy mandates and the state privacy law and regulations.

A number of outreach and communication efforts will be investigated, including:
- Face-to-face training
- Community forums
- Teleconference
- Webex conferences
- Newsletters
- Web posted news and alerts
- Brochures
- Mass media

The education package may be posted on a stakeholder community member's website for use and download—at minimum information will be available and accessible.

6.1.5 Business agreements, and uniform patient consent/authorization forms

Uniform patient consent and consent management, or authorization, is outlined above. Business agreements will be discussed during the first phase of the implementation of the Massachusetts plan.

6.2 Solutions to issues derived from state privacy and security laws/regulations

- Solutions that would require changes in existing state law/regulations, e.g., draft model legislation
- Solutions that would require new state laws/regulations
- Solutions that would address issues of non-compliance with state laws/regulations
- Education solutions to address misinterpretations of state laws/regulations

MA-HISPC solutions areas represented by the four bullets above are outlined in the legal, policy and educational solutions of this Report. See section 6.1 above.

The RTI review of the MA-HISPC interim analysis of solutions report stated "legislative and regulatory solutions should have been identified but noted as solutions that were 'not on the table' at this time."

In Massachusetts, the Executive Office of Health and Human Services (EOHHS) controls 50% of the state's budget. EOHHS is a major member of the MA-HISPC project and all other health care projects within Massachusetts. This—coupled with MHDC's almost 30 year history—permits the healthcare industry to solve many issues practically and pragmatically.

Further, in MA-HISPC Interim Implementation Planning Report submitted on February 14, 2007, there is a more nuanced answer to this question. There are places within the state's healthcare regulations where it may be possible to address consent management issues, especially to deal with sensitive information.

The Implementation Project outline includes monitoring changes in the state's healthcare law and encouraging the medical society, the hospital association, the Massachusetts Bar Association, and the Boston Bar Association to work collaboratively on many of these issues.

6.3 Solutions to issues driven by intersection between federal and state laws/regulations

- Solutions applicable to general privacy/security federal laws and regulations (e.g. HIPAA Privacy, HIPAA Security)
- Solutions applicable to state programs (e.g., Medicaid)
- Solutions that would address issues of non-compliance with federal laws/regulations (such as non-compliance with HIPAA Privacy, HIPAA Security)
- Education solutions to address misinterpretations of federal laws/regulations

MA-HISPC solutions areas represented by the four bullets above are outlined in the legal, policy and educational solutions of this Report. See section 6.1 above.

6.4 Solutions to Enable Interstate e-Health Information Exchanges

MA-HISPC solutions affecting interstate Health Information Exchange are outlined below, Section 7.

7.0 National-level Recommendations

The focus of this project is on solutions that the states and stakeholders can implement at the organization, local, or state level to develop privacy policy and security standards that will enable eHIE on a nationwide scale. However, it is recognized that states and stakeholders may have recommendations for the federal government that could be of value to states as they grapple with the development of privacy policy and security standards. These type of recommendations will be recorded, and may include requests for guidance from the Office of Civil Rights on HIPAA Privacy and Security requirements. Any recommendation in this section will provide detailed examples of the issues and explain why federal involvement is the only recourse.

MA-HISPC stakeholders want to work with our sister states and the territories to solve cross-border issues such as state law and regulation differences, especially in the areas of consent, sensitive information, and routine and emergency public health information sharing. One New England state HISPC project has already approached the MA-HISPC project to begin work and coordination during the HISPC IPWG phase.

MA-HISPC suggests that the states and territories work with the National Conference of Commissioners on Uniform State Laws. A number of the MA-HISPC stakeholders have expressed interest in working with such a project specific to patient consent management and sensitive information management.

MA-HISPC suggests that the HIPAA privacy requirements for minimum necessary, de-identification, limited data set, and designated data set be reviewed for possible technical adjustments. MA-HISPC suggests that the Department of Health and Human Services develop updated, and more detailed guidance for these HIPAA privacy requirements either informally or through the notice and comment process. For example:

1. Providers think that they need to do a minimum necessary review for treatment purposes.
2. Across the industry, people speak of de-identified data and do not understand that more than a few data elements may be removed from the information; the term de-identification seems to be a shorthand term that is developing a life of its own.
3. People do not understand that they may be speaking of a limited data set when they use the term de-identified; the term and parameters of a limited data set are not understood.
4. Providers still do not understand that a limited data set needs to include the information from outside their practice or office or facility and that it may be used to make medical decisions

MA-HISPC suggests that the states and the territories continue to work together at the end of the HISPC project, possibly with or through the National Governors Association (NGA) or the NGA's eHealth Alliance**.** However, MA-HISPC is concerned about confusion that federal contracts and initiatives may be causing the states and the industry. For example the use cases/ scenarios are different between AHIC, HISPC and other work. What will the NGA e-Health State Alliance create that adds to or helps resolve the confusion?

8. Conclusions and Next Steps

8.1 Key Findings Informing Next Steps

MA-HISPC's implementation plan is informed by several key findings of our work to date:

- Any follow-on implementation work that happens as a result of the MA-HISPC project must be informed by what is currently underway and planned in the Commonwealth. In other words, the MA-HISPC project and any successor project(s) should not reinvent the wheel. Thus, the first step in the MA-HISPC implementation plan is to inventory all the interoperability work from the recent past, currently underway, and planned for the immediate future.
- No HIE or interoperability project can be established and progress until it is determined what clinical data will be shared, why the data will be shared, and how the data sharing will happen. This determination will be made by forming a Clinical Working Group convened for this specific purpose. Its findings and recommendations will form the foundation of any interoperability project. This is where the discrete use case will be discussed and outlined. It is anticipated that use cases will include mental health information scenarios.
- It has also become apparent in the IPWG meetings that the Education solution introduced in the MA-HISPC Interim Analysis of Solutions Report should include the concept and work of Communications separate and distinct from Education.
- The project work highlights the need to include patients/consumers and patient advocacy groups in all ongoing work. The best way to obtain patient and consumer understanding and buy-in is to include them at the beginning of a project. The MA-HISPC implementation plan will include patients, consumers and patient consumer advocacy groups in all committee and task force work outlined below.
- Legal analyses (compilation of laws and regulations)

As the IPWG discussed the MA-HISPC project implementation plans, a number of terms used imply that any HIE and interoperability project is not a linear set of events or tasks or work. The work is iterative, nested, cumulative, and additive. In other words, the MA-HISPC implementation strategy must be dynamic enough to change and grow as the project develops and progresses.

8.2 HISPC Opportunity and Implementation Plan Outline

The HISPC project has provided Massachusetts with an opportunity to: increase the scope and depth of stakeholder input on the statewide stage—including a key objective for greater consumer participation; confirm the value of continuing MHDC process to collaborate around critical issues that—once solved—move HIE forward; and identify needs and priorities to plan for policy and procedure development to support further HIE achievements.

The MA-HISPC implementation plan cites as a priority the need for a consent management project for the state that will focus on the critical areas of patient consent management for general and sensitive clinical information. The plan describes a statewide constituent structure to support a federated framework for addressing the most commonly needed provider use cases for clinical data exchange. MA-HISPC plans to describe a project that will focus on:

- Identifying critical use cases where providers need improved workflow for reasons including: frequency, complexity of information transfer, and/ or time consumption.
- Collecting the inventory of existing policy, procedure and practices around these use cases.
- Confirming the laws, regulations, etc. affecting these use cases.

- Communicating and educating all stakeholders, including consumers on this policy development process.

8.3 Background Discussion

Upon review in preparation for developing the Implementation Plan Report it was determined that two large projects are necessary first steps, each of which has multiple components. Based on stakeholder input, the priorities for MA-HISPC implementation planning are the development of specifications that address issues surrounding the consent[5] management and sensitive information management. A consistent finding through the HISPC process has been that different stakeholder types and representatives from the healthcare community manage HIE with different interpretations of HIPAA, other federal laws, and state laws and regulations. The implementation process described in this report will bring the healthcare community toward consensus on legal, policy and operational guidelines. Additionally, the need to identify viable and useful communication strategies at every point in the implementation process has been emphasized with recommendations to address as soon as practical.

Simply posed, the questions that need to be fully addressed are: How to obtain patient consent for participation in an HIE network? Where, how and when should it be collected? How can mental health, or other sensitive clinical information be rolled into general consent workflow for participation in an HIE network? The MA-HISPC Project sees creation of policies and procedures in these two critical areas to be both a practical starting point and a significant contribution to the national level of HIE networking.

In conversations with many other states working on this HISPC project, the MA-HISPC team has learned that patient consent and sensitive clinical information are also of major concern. It seems imperative that both our state and the nation solve these issues before a HIE network can be implemented and/or will work efficiently.

Consent Management in Health Information Exchange

Stakeholder interviews revealed uncertainty in applying state privacy law (beyond the "sensitive health information laws") and best practices to health information exchange between organizations. Key issues include varying interpretations of the need for consent—for the use of patient information in HIE systems, applying privacy laws to various models of HIE (pull systems, messaging systems, and others), the best method for recording and communicating patients' preferences, and the privacy implications of record locator services and similar technologies. Until these uncertainties are addressed in a clear and uniform way, they will be barriers to the development of local and regional information networks that protect patient privacy in an appropriate manner.

Sensitive Health Information

[5] Consent in this document means patient permission for use of PHI within the normal flow of treatment, payment and health care operations, both within paper and electronic environments; it does not mean informed consent for a medical procedure or treatment

MA-HISPC project discovered that the sensitive information issues are pervasively embedded within the consent issue. Complying with Massachusetts' laws governing specific types of health information, including mental health records and medication lists, genetic test results, HIV-AIDS test results, and several others, were consistently identified as points of concern and difficulty in exchange of health information. Similar concerns were expressed regarding compliance with federal substance abuse record regulations. Stakeholders need solutions that facilitate appropriate exchanges for health information while preserving important privacy values and consumer protections.

8.4 MA-HISPC Statewide Strategy and Nationwide Utility

MA-HISPC IPWG recognizes that the development of HIE and interoperability standards must continue on the national level. However, the development of many standards is delayed or blocked by the lack of policy decisions that integrate legal requirements into the practical questions that face HIE networks. The MA-HISPC project has benefited from the insight and input of the 2006-2007 HITSP Chair as a member of the Steering Committee and IPWG. Recommendations were received to develop project plans that begin first to form policies and procedures as the foundation for widespread consensus, education and communication strategies for Massachusetts stakeholders and constituents. In addition, recommendations were received to provide the needed definition at the national level for more additional standards development in the year 2007. The IPWG agreed that this implementation phase is an appropriate place to begin this work.

8.5 Conclusion

While many components useful for technology development were collected and documented during the variations and solutions working sessions, it is felt that policy development leading to an operational framework will provide the critical starting point. Administrative specifications and technical architecture to advance HIE interoperability, while essential, were not seen as viable projects for the short-term next steps envision by MA-HISPC at this time. To this point: policies to guide consistent process for patient consent, authorizations and/or permissions are needed prior to standardization of consent metadata and/or consent documents for EHR use cases; policies for special treatment of selected lab results such as genetic testing, HIV, drug levels, alcohol levels, etc., could be included in these patient privacy considerations; policies for restriction of selected medications; and the challenging policy for consistent interpretation of HIPAA privacy provisions for minimum necessary data—all are needed in the near term for HIE momentum

The implementation project will include a Steering Committee, and Clinical, Legal, Technical, Policy, Multi-state, Education, and Communication working groups.