MARYLAND

Health Information Technology State Plan

FY 2011 – FY 2014

Appendices

MHCC MARYLAND HEALTH CARE COMMISSION

Commissioners

Marilyn Moon, Ph.D., Chair

Vice President and Director, Health Program
American Institutes for Research

Garret A. Falcone, Vice Chair
Executive Director
Charlestown Retirement Community

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

John E. Fleig, Jr.
Director
United Healthcare

Tekedra McGee Jefferson, Esquire
Assistant General Counsel
AOL, LLC

Kenny W. Kan
Senior Vice President, Chief Actuary
CareFirst BlueCross BlueShield

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

Robert Lyles, Jr., M.D.
Medical Director
LifeStream Health Center

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

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

Kurt B. Olsen, Esquire
Klafter and Olsen LLP

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

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

Adam Weinstein, M.D.
Medical Director
Nephrology and Transplant Services
Shore Health System

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

Appendices

To access the all other sections, click here

Appendix A
MSO State Designation Criteria

Maryland Health Care Commission

Management Service Organizations
State Designation Criteria

Table of Contents

OVERVIEW

Utilizing health information technology (health IT) in an optimal manner can help improve health care quality, prevent medical errors, and reduce costs by delivering essential information at the point of care. Successful health IT requires two crucial components – widespread use of electronic health records (EHRs) and the ability to exchange health information privately and securely. While both are challenging projects conceptually, technologically, and economically, the implementation of EHRs poses special challenges. These challenges mostly relate to the cost of the software and maintaining systems that support the application. The integration of EHRs into a physician practice takes time and is influenced by technological constraints, costs, and different perceptions and expectations. Management service organizations (MSOs) have emerged as a way to address these challenges.

MSOs offer centralized administrative and hosted technology services and are considered a viable alternative to the traditional EHR client-server model where the technology is maintained locally at the provider site. MSOs enable physicians to access patient records wherever access to the Internet exists. These organizations are capable of supporting multiple EHR products at reduced costs through economies of scale and bulk purchasing. Technical support usually extends beyond the standard business hours and in some instances is available on a 24/7 basis. Data is safeguarded through a network operating center that, by design, ensures high quality and uninterrupted service. Remotely hosted EHRs enable providers to focus on practicing medicine rather than dedicating staff to support the application and technology.

On May 19, 2009, Governor Martin O'Malley signed into law House Bill 706, *Electronic Health Records – Regulation and Reimbursement*. This law requires the Maryland Health Care Commission (MHCC) to designate one or more MSOs that offer EHRs throughout the state by October 2012. The MHCC convened an MSO Advisory Panel that developed the criteria for *State Designation*. The criteria outline the requirements for *MSO State Designation* and assess privacy and confidentiality, technical performance, business practices, resources, security, and operations of MSOs.

STATE DESIGNATION I: QUALIFYING EVENTS

MSOs will need to conform to select requirements in order to be considered for State Designation. The requirements and the Criteria are subject to change and existing State Designated MSOs that seek to renew their State Designation must meet the requirements in existence at the time of application.

- The MSO must offer a hosted EHR solution that is certified by a nationally recognized certifying organization.
- The MSO must complete an application and self-assessment manuscript using the Criteria recognized by the MHCC.
- The MSO and any subcontractor must provide services (i.e., education, technology, support, etc.) using a workforce where at least 50 percent of the resources originate in Maryland.
- The MSO must establish and maintain an active connection to the state designated health information exchange.
- The MSO must agree to a bi-annual site visit.
- The MSO must re-apply every two years and meet the requirements outlined in the MSO State Designation Criteria.
- The MSO must support state efforts and the efforts of the state designated health information exchange in advancing health information technology consistent with the goals of the Office of the National Coordinator for Health Information Technology.

STATE DESIGNATION II: PRIVACY AND CONFIDENTIALITY

State Designated MSOs must have appropriate policies and procedures in place that comply with the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) requirements to ensure the integrity and confidentiality of protected health information (PHI). These policies and procedures must protect against any anticipated threats or hazards to the security or integrity of electronic information. The policies and procedures must also protect an individual's interests by managing who has access to PHI. The measures stated below reference specific information that should be discussed in the self-assessment manuscript.

MEASURES TO ENSURE DATA PRIVACY AND CONFIDENTIALITY

- The MSO must have policies to protect against inappropriate disclosure of PHI.
- The MSO must have policies and procedures in place to ensure continuing compliance with data security standards, including secure methods of access to and transmission of data.
- The MSO must refrain from selling, marketing or otherwise using PHI in any way that violates privacy or confidentiality.
- The MSO must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any federal or state legislation.
- The MSO must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software and/or intrusion events.
- The MSO must maintain a list of all individuals, contractors, and business associates with access to electronic PHI maintained by the MSO.
- The MSO must demonstrate that configuration standards are in place and include patch management for systems that store, transmit, or access electronic PHI, including workstations within the MSO.
- The MSO must implement policies and procedures to ensure compliance with any applicable federal and state privacy and security requirements.
- The MSO must notify their customer(s) in writing within 60 calendar days of discovering a breach or disclosure of PHI.
- The MSO must have policies and procedures to ensure that PHI is not stored nor transported in an insecure manner as established by federal and state security requirements.

STATE DESIGNATION III: TECHNICAL PERFORMANCE

State Designated MSOs must provide assurances and have policies in place to ensure that authorized users are able to access patient health records in a timely manner. Areas of technical performance include:

- Customer service inquiries
- System availability
- Compliance with industry standards
- Capacity monitoring and management
- Auditing
- Storage and retrieval
- Internet access

CUSTOMER SERVICE INQUIRIES

- The MSO must have a service inquiry management and a tracking system that documents date and time of initial contact through resolution.
- The MSO must have the capability to acknowledge inquiries within three business hours.
- The MSO must respond to open inquiries within one business day with either a resolution or plan of action for issues requiring escalation.
- The MSO must have documented escalation procedures based on severity to follow the inquiry to completion.

SYSTEM AVAILABILITY

- The MSO must have minimum system availability and appropriate redundancy that assures system access for 98 percent of contracted and/or advertised hours. This requirement shall not preclude acts of nature.
- The MSO must support extended hours of support, if required by clients.
- The MSO must provide practices with a notice of all scheduled downtime at least one business week prior to the actual downtime.
- The MSO must notify all practices within two hours in the event of unscheduled downtime.

COMPLIANCE WITH INDUSTRY STANDARDS

- The MSO must maintain a current analysis of any federal and state privacy or security laws that the MSO reasonably believes apply to information stored or transmitted by the MSO (e.g., security breach notification laws), and the MSO must have a plan to comply with any such laws.

CAPACITY MONITORING

- The MSO must have the ability to measure system capacity and have an ongoing monitoring capability in place for measuring that system and managing capacity.

- The MSO must have a formal system capacity plan for handling load and expansion including a demonstration of 99.5 percent availability on communication exchange components per the advertised service level agreements. This requirement does not preclude acts of nature.

AUDITING

- The MSO must implement an accurate and transparent auditing mechanism.

STORAGE AND RETRIEVAL

- The MSO must have an off-site location that has a six-month minimum backup archive, storage and retrieval of all data, and adheres to all applicable federal and state regulations.

- The MSO must annually test the backup restoration process for all practice data.

- The MSO must have, or show progress towards having, a seven-year back-up archive, storage and regeneration capabilities at minimum, and a process for providing extended back-ups at the request of the practice.

- The MSO must have the ability to partition data into separate files that can either be aggregated for a multi-provider practice or separated for extraction by a single provider of that multi-provider practice.

- The MSO must have a process in place to have operations restored in a timely manner.

INTERNET

- The MSO must have a firewall configured to protect the system integrity.

- The MSO must ensure that internal databases cannot be modified directly through an external website, unless made securely, by authenticated users and contain integrity checks.

- The MSO must ensure that integrity checks are made on all modifications to external systems (e.g., those kept on the web server) prior to synchronization with any internal database.

- The MSO must provide capacity and bandwidth adequate for business needs. The MSO must have a process in place to daily monitor Internet bandwidth and communication server performance.

- The MSO must have processes and procedures in place to monitor and/or block intrusion attempts or attacks from the Internet and provide alarms to appropriate personnel.

- The MSO must have documented procedures to respond to a successful intrusion or attack from the Internet within a timely manner of when an alarm is generated or notification received.

- The MSO must have an established plan to conduct an annual threat and vulnerability assessment through an independent third party. The MSO must develop an improvement process based on the results of those assessments.

- The MSO must have documented web server security configurations to protect the web server from attack or intrusion.

STATE DESIGNATION IV: BUSINESS PRACTICES

State Designated MSOs must have sound business practices that support the goals of the organization. These business practices center on procedures for measuring customer satisfaction; provide non-restricted access to the system based on assigned level of access; adequately provide for customer education and training; and have standard contracts and service agreements.

TRUTH-IN-ADVERTISING

- The MSO must demonstrate compliance with their published service levels.

ACCESS

- The MSO must offer at least one nationally certified hosted EHR solution.

AGREEMENTS

- The MSO must have service level agreements that take into consideration the needs of the MSO and practice, and have reasonable termination provisions for both parties.

STATE DESIGNATION V: RESOURCES

State Designated MSOs must possess the physical, human, and administrative resources necessary to maintain a high level of technical performance and business practices. These resources must include facilities adequate to conduct the MSOs current and anticipated business volume and maintain qualified staff.

PHYSICAL RESOURCES

- The MSO must have physical resources adequate for accomplishing the stated mission.
- The MSO must regularly monitor capacity to support its defined services.
- The MSO must have a formal expansion plan in place when strategic plans project organizational growth of more than 10 percent annually.

PERSONNEL

- The MSO must have sufficient, qualified personnel to perform all tasks associated with accomplishing the stated mission.
- The MSO must ensure that employees receive effective, relevant job training to remain current in knowledge and skills.
- The MSO must provide, at a minimum, annual job training that includes training applicable with the HIPAA provisions for all employees and ensure contractors have received similar training.
- The MSO must maintain a record of employee and contractor compliance with the routine training. A copy of the curriculum, and any versioning, must also be kept on file.
- The MSO must demonstrate a thorough due diligence process in their hiring practices.

STATE DESIGNATION VI: SECURITY

State Designated MSOs must have appropriate administrative, technical, and physical safeguard policies and procedures to ensure the integrity and confidentiality of PHI. These policies and procedures must protect against any anticipated threats or hazards to the security or integrity of the data. MSOs must comply with all the HIPAA requirements. MSOs should uniquely describe their policies in the self-assessment manuscript relating to the following:

ADMINISTRATIVE SAFEGUARDS

- The MSO must comply with all federal and state security rules.
- The MSO must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the MSO.
- The MSO must implement an enforcement policy that will authorize the MSO to apply appropriate sanctions against workforce members (i.e., employees, contractors, and vendors) who are not in compliance with the MSO's security policies and procedures.
- The MSO must implement procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports.
- The MSO must maintain a record of any discrepancies noted from the record review and report these discrepancies to the security officer for review.
- The MSO must implement policies and procedures to ensure that all members of the MSO's workforce have access to the minimum necessary PHI to perform work assignments and to prevent access to workforce members who do not need access electronic PHI.
- The MSO must implement termination procedures for withdrawing access to PHI when the employment of a workforce member ends.
- The MSO must implement and document a security awareness and training program for all members of the MSO's workforce.
- The MSO must implement and document procedures for creating, changing, and safeguarding passwords and/or other login procedures.
- The MSO must have a process in place to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents that are known to the MSO.
- The MSO must establish written policies and procedures for responding to an emergency or other occurrence such as fire, vandalism, system failure, or natural disasters that impact systems that contain PHI.

- The MSO must include in their disaster recovery/business continuity plan the following: annual testing of the plan, what constitutes a disaster, a communication plan notifying providers of the disaster and escalation process, and identification of critical personnel who are responsible for conducting the damage assessment and mitigation process.

- The MSO must implement and document procedures for periodic testing, assessment, and review and revision of contingency plans. Testing and all appropriate revisions must occur no less than annually.

PHYSICAL SAFEGUARDS

- The MSO must implement and document policies and procedures to limit physical access to its information systems and the facility or facilities in which they are housed, while also providing that all properly authorized persons have adequate access.

- The MSO must establish procedures that allow secure facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

- The MSO must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

- The MSO must implement procedures to control and validate a person's access to data based on their role or function.

- The MSO must implement policies and procedures, including a log, governing the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility.

- The MSO must implement policies and procedures to address the final disposition of PHI and the hardware or electronic media on which it is stored.

- The MSO must implement procedures for removal of PHI from electronic media before the media are discarded or made available for re-use.

TECHNICAL SAFEGUARDS

- The MSO must implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.

- The MSO must assign a unique name and/or number for identifying and tracking all system user identities.

- The MSO must establish procedures for accessing necessary PHI during an emergency.

- The MSO must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

- The MSO must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.

ORGANIZATIONAL REQUIREMENTS FOR BUSINESS ASSOCIATE CONTRACTS

- The MSO must require Business Associates to implement administrative, physical, and technical policies and procedures that are reasonable, appropriate, and required by federal and state regulations to protect the confidentiality, integrity, and availability of the PHI it creates, receives, maintains, or transmits on behalf of the MSO.

- The MSO must require Business Associates to report to the MSO any security incident of which it becomes aware.

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

- The MSO must record and maintain the policies and procedures implemented to comply with applicable federal and state regulations; policies and procedures should be available to those that need access to them.

- The MSO must review documentation annually, and update as needed, in response to environmental or operational changes affecting the security of the PHI.

STATE DESIGNATION VII: OPERATIONS

State Designated MSOs are required to support the activities of the Regional Extension Center. The leading areas of support center on EHR implementation support, technical assistance, and ongoing assistance to the provider to meet the *meaningful use* requirements established by the Centers for Medicare & Medicaid Services.

- The MSO must have an EHR adoption education plan for providers without an EHR system.
- The MSO must have a plan for maximizing EHR functionality of providers with an EHR system.
- The MSO must have a plan in place to furnish technical assistance to the providers participating with the MSO.
- The MSO must conduct an annual provider satisfaction survey under the guidance of the Regional Extension Center and in consultation with the MHCC and report on the findings.

APPENDIX

Acknowledgements

The Maryland Health Care Commission greatly appreciates the contribution made by everyone that participated in the Advisory Panel and the ongoing support in developing the criteria for state designation. Special thanks go to the following individuals for giving of their time to complete the designation criteria. The information provided by these individuals has led to this groundbreaking initiative.

Doug Abel
Anne Arundel Medical Center

Ray Adkins
Peninsula Regional Medical Center

Scott Afzal
Audacious Inquiry

Salliann Alborn
Community Health Integrated Partnership

Jama Allers
The Maryland State Medical Society

Karen Barker
LifeBridge Health

Lee Barrett
EHNAC

Shelby Boggs
NextGen Healthcare

Gary Broadwater
Antietam Health Services

Jeffrey Cheng
GURU Consulting

Chuck Dorin
e-MDs

Kathryn Feldmann
CGI System Integrators

Mike Fierro
Dynamed

Marty Frygier
Perficient

Beverly Gazmen
Chesapeake Ortho & Sports

Ed Grogan
Calvert Memorial

Chuck Henck
University Physicians, Inc

Michael Hill
SysInformation

David Horrocks
CRISP

Clay House
CareFirst

Scott Inter
Calvert Memorial

Steve Johnson
MedChi

Mary Jane Kamps
Union Hospital of Cecil County

Jennifer King
Solomon Eye Physicians

Barbara Klein
Concordant

Traci La Valle
Maryland Hospital Association

Darren Lacy
Johns Hopkins

Bel Leong-Hong
Knowledge Advantage

Ron Moser
EHNAC

Minh Nguyen
Millennium Enterprise

Dave Palmisano
Sandlot

David Quirke
Frederick Memorial Hospital

Denise Reeser
New Heights Consulting

Ewart Russell
Children's Pediatric Associates

Telly Shackleford
Sandlot

Michael Snyder
Planned Systems International

Matthew Tan
Knowledge Advantage

Kevin Tyler
Mid-Atlantic Systems

Tina Whims
Frederick Health Services

Gary White
Practice Works Systems

Appendix B
State Designated MSOs

State Designated Management Service Organizations – Candidacy Status									
Count	MSO	Contact Name	Address	City	State	Zip	Phone	Email	EHR
1	A&T Systems, Inc.	Fred Sanders	12200 Tech Road	Silver Spring	MD	20904	(301) 384-1405	fred.sanders@ats.com	eClinicalWorks
2	Adventist HealthCare	Arumani Manisundaram	1801 Research Blvd. Suite 400	Rockville	MD	20850	(301) 315-3000	amanisun@adventisthealthcare.com	eClinicalWorks & Allscripts
3	*Anne Arundel Medical Center	Doug Abel	2001 Medical Parkway	Annapolis	MD	21401	(443) 481-5215	dabel@aahs.org	Epic Systems
4	*AVS Medical	Lloyd Morris	877 Balto. Annapolis Blvd. Suite 111	Severna Park	MD	21146	(410) 975-9160	lloyd@avsmedical.com	McKesson Practice Partner
5	Business Engineering, Inc.	Jonathan Krasner	11130 Sunrise Valley Drive Suite 202	Reston	VA	20191	(703) 582-8300	jonathan.krasner@beinetworks.com	Greenway Medical
6	*Children's IQ Network	Brian Jacobs	111 Michigan Avenue, NW	Washington	DC	20010	(202) 476-3969	bjacobs@cnmc.org	eClinicalWorks & Sage Intergy
7	*CHIP	Salliann Alborn	802 Cromwell Park Drive Suite V	Glen Burnie	MD	21061	(410) 761-8100	salborn@chipmd.org	GE Centricity
8	*D'Souza & Associates	Rohit D'Souza	530 Schoolhouse Road Suite A	Hockessin	DE	19707	(302) 239-9671	rohit@dsouzainc.com	Sage Intergy
9	*Erickson IT	Scott Erickson	12864 Macbeth Farm Lane	Clarksville	MD	21029	(410) 929-5570	scott@ericksonit.com	GE Centricity
10	*Frederick Memorial Hospital	Tina Whims	478 Prospect Boulevard	Frederick	MD	21701	(240) 379-6061	twhims@fmh.org	NextGen
11	*GBMC	Tressa Springmann	6701 North Charles Street	Baltimore	MD	21204	(443) 849-3749	tspringm@gbmc.org	eClinicalWorks
12	MedChi Network Services, LLC	Gene Ransom	1211 Cathedral Street	Baltimore	MD	21201	(410) 539-0872	gransom@medchi.org	Allscripts
13	*MedPlus	Scott Lentz	4690 Parkway Drive	Mason	OH	45040	(513) 204-2625	slentz@medplus.com	MedPlus Care360
14	*Mosaic Technologies	Jason Bach	15720 Crabbs Branch Way Suite 2B	Rockville	MD	20855	(240) 399-3900	jbach@mosaictechnologies.com	gloStream & McKesson
15	Mid-Medical Contractor Teaming Arrangement	Kevin Tyler, Sr	8377-R Piney Orchard Parkway	Odenton	MD	21113	(410) 551-9815	Kevin.Tyler@mascc.com	Praxis & eClinicalworks
16	*Networking Technology RxNT	Karen Childs	1106 West Street	Annapolis	MD	21401	(800) 943-7968	kchilds@rxnt.com	RxNT EHR
17	SuccessEHS	Adele Allison	One Metroplex Drive Suite 500	Birmingham	AL	35209	(205) 949-1322	adelea@successehs.com	SuccessEHS
18	*Sydian Solutions, Inc.	Chuck Dorin	9505 Hull Street Road Suite C	Richmond	VA	23236	(804) 276-6456	cdorin@sydian.com	eMDs
19	*Wavelength	Murray Oltman	504 Franklin Avenue PO Box 739	Berlin	MD	21811	(410) 629-0913	murray@wavelengthIS.com	Allscripts
20	*Zane Networks, LLC	Luigi Leblanc	8070 Georgia Avenue Suite 407	Silver Spring	MD	20910	(301) 560-0500	leblanc@zanenetworks.com	Sevocity & MIE EHR

**Denotes participation with the Maryland Regional Extension Center*

Rev. 2/3/2011

Appendix C

Approved Policies, Proposed Policies & Primary Reviewers

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange

Approved Policies, Proposed Policies & Primary Reviewers

The table below details approved policies and a prioritization of proposed policies for the statewide health information exchange. The status of the proposed policies, the Policy Board member that volunteered to be the Primary Reviewer of each policy, and their respective organizations are listed.

Approved Policies	Approval Date	Review Date
Participating Organization Access v2.0	11/09/10	11/09/11
Consumer Choice v2.0	1/11/11	1/11/12
User Authentication v2.0	1/11/11	1/11/12
User Authorization v2.0	11/09/10	11/09/11

Proposed Policies	Status	Primary Reviewer	Organization
Sensitive Health Information	v1.2.3	Sarah Tucker	National Network to End Domestic Violence
Emergency Access for Participating Organizations	v1.2.2	Sarah Tucker	National Network to End Domestic Violence
Suspension and Termination of User Access	v1.2.1	Doug Abel	Anne Arundel Medical Center
Data Use and Disclosure	v1.1	Chris Shea Peggy Leonard	OSI – Baltimore Genesis Healthcare
Consumer Access	v1.0	Steve Daviss Salliann Alborn	Baltimore Washington Medical Center Community Health Integrated Partnership
Audit	v1.0	Shannah Koss	Koss on Care
Consumer Access to Audit	v1.1	Liza Solomon	Consumer Member
Complaints	v1.1	Ellen Maltz	M&T Bank
Notification of Breach	v1.1	Damien Doyle	Hebrew Home of Greater Washington
Public Health Reporting	v1.0	Frances Phillips Liza Solomon	DHMH Consumer Member
Suspension and Termination of Consumer Access	v1.0	Lee Cotton	Higher Ground, Inc.
Consumer Outreach & Education	v1.0	Shannah Koss	Koss on Care
Enforcement	v1.0	TBD	TBD
Policy Review & Revisions	v1.0	TBD	TBD
Liability	v1.0	TBD	TBD
Cyber Security	v.1.0	TBD	TBD
Portable Devices and Removable Media	v1.0	TBD	TBD

Policy Status Key	
v1.0	First Draft
v1.1	First Draft with Primary Reviewer Comments
v1.2	Draft Iterations *(i.e., 1.2.1, 1.2.2, 1.2.3, 1.2.4, etc.)*
v1.3	Final Draft
v2.0	Approved by Policy Board

Appendix D
HIE Adopted Policies

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange

CONSUMER CHOICE	
Approval Date: *01-11-11*	Scheduled Review Date: *01-11-12*

Goal: The *Consumer Choice* policy aims to ensure that all consumers[1] are afforded the opportunity to control the use of their protected health information (PHI) that is available through the statewide health information exchange (HIE). Allowing consumers the ability to control their information that can be queried is a vital component of a trusted, consumer-centric statewide HIE. As technology continues to evolve, the state designated HIE must explore and implement the ability for consumers to control the access of their PHI at a more granular level. This may include limiting access by categories of medical data, specific encounters, or classification of providers.

Purpose: This policy describes the state designated HIE's responsibility as it relates to a consumer's choice in allowing their PHI to be made available through the statewide HIE. This will enable consumers to control who has access to their electronic health information, and allow them the opportunity to choose whether and when to participate in the statewide HIE. This policy will ensure that the PHI of consumers who choose not to participate will not be available for query through the statewide HIE.

Policy:

1. The state designated HIE must allow consumers the ability to opt-out[2] of the statewide HIE, and to reverse their opt-out decision. All consumers are considered to be a participant in the statewide HIE until they have explicitly opted-out. The state designated HIE must allow consumers the ability to communicate their preference through an appropriate medium of the consumer's choice. The state designated HIE is responsible to make available patient education information designed to assist consumers to exercise an educated choice regarding participation in the HIE.

2. The state designated HIE must require participating organizations to inform the consumer of their right to object prior to any initial query of the consumer's PHI through the statewide HIE, except in a medical emergency.[3] Participating organizations must refrain from querying the consumer's PHI through the statewide HIE if the consumer objects.

3. The state designated HIE must provide consumers with the option to receive confirmation of their choice to opt-out or back into the statewide HIE. If confirmation is requested, the state designated HIE must acknowledge on a timely basis the change in participation status through an appropriate medium of the consumer's choice. The state designated HIE must include in the opt-out information an explanation of when the change will become effective and what information will be excluded from the HIE.

---

[1] A consumer is an individual that is capable of making decisions regarding their health care as defined by existing law, or a parent/legal guardian.
[2] Opt-out is when a consumer elects to prevent their PHI from being made available through the statewide HIE.
[3] Once permission to query is given it may be relied upon at future encounters.

4. The state designated HIE will ensure that consumer PHI is not available for query when a consumer has opted-out of the statewide HIE. A consumer's request to opt-out must become effective not later than one (1) business day from the day that the opt-out request is received by the state designated HIE. Consumers must be allowed to modify their participation in the statewide HIE at any time and through various methods.

5. The state designated HIE will maintain a Master Patient Index (MPI) that contains a minimum data set to identify consumers and their current opt-out status.

6. The state designated HIE will maintain an audit trail that uniquely identifies a consumer's participation status for a length of time consistent with state and federal requirements. The information must be housed in a retrievable storage medium. The state designated HIE is required to perform periodic testing to demonstrate that stored data is recoverable.

7. The state designated HIE must provide consumers, upon request, with a report related to who has accessed their PHI through the statewide HIE. Consumers may request and receive a report free of charge twice yearly. The statewide HIE may charge a reasonable fee for any additional reports.

Procedure:

The state designated HIE should implement procedures that are inclusive of the following items:

1. The state designated HIE should allow a consumer to select their participation status related to opting-out or back into the statewide HIE in at least six (6) ways:

    a. Online via a secure website, which should be available 24 hours per day (except for reasonable maintenance down-time);

    b. A toll-free number, which should be available Monday through Friday;

    c. By mail, via a standardized form;

    d. By fax, via a standardized form;

    e. In person at the state designated HIE during business hours; or

    f. Through a willing participating organization acting on the consumers behalf.

2. The state designated HIE should make materials available to participating organizations to use to educate consumers about the statewide HIE and their participation options. Participating organizations should make these materials available to consumers and discuss the materials with them at their initial visits.

3. The state designated HIE should make changes to a consumer's participation status selection at the HIE level within (1) business day of receipt.

4. In the event that a consumer requests a change in their participation status, the state designated HIE should confirm that the participation status was changed within three (3) business days. Consumers should be offered at least five (5) ways to receive this notification:

    a. Online to an email specified by the consumer;

    b. A letter to an address specified by the consumer;

    c. A letter by fax to a fax number specified by the consumer;

    d. A letter in person at the HIE during normal business hours;

    e. Via a text message.

5. The state designated HIE should establish a process to validate guardianship.

6. The state designated HIE should offer consumers a copy of who has accessed their PHI via the statewide HIE upon request, free of charge, twice yearly. The state designated HIE may charge a fee for additional requests, which cannot exceed cost.

Associated Policies:

1. *Consumer Access*
2. *Consumer Access to Audit*
3. *Consumer Outreach & Education*
4. *Exceptions to Consumer Choice*
5. *Sensitive Health Information*
6. *Suspension and Termination of Consumer Access*

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange

PARTICIPATING ORGANIZATION ACCESS	
Approval Date: *11-09-10*	Scheduled Review Date: *11-09-11*

Goal: The *Participating Organization*[1] *Access* policy aims to ensure that only authorized users have access to the minimum necessary[2] information through the statewide health information exchange (HIE) that is limited to authorized purposes and relevant to their current role as defined by the participating organization. The standards for minimum necessary are established by the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) Administrative Simplification Provisions.

Purpose: This policy describes the state designated HIE's responsibilities as it relates to allowing participating organizations the ability to access information through the statewide HIE. The state designated HIE is responsible for ensuring that policies related to *Participating Organization Access* are implemented according to the provisions outlined in this policy.

Policy:

1. The state designated HIE must require users to be authenticated according to the *User Authentication* policy prior to accessing protected health information (PHI) through the statewide HIE. Proper authentication will ensure that only appropriately authorized users have access to the HIE.

2. In consultation with stakeholders, the state designated HIE will develop and maintain an HIE Access Matrix. The HIE Access Matrix must be reviewed annually to determine if revisions are necessary to accommodate changes in technology, standards, and laws. The HIE Access Matrix must remain constant across all participating organizations.

3. The state designated HIE will include in the HIE Access Matrix defined levels of access to the statewide HIE that are available to appropriately authorized users for authorized purposes. The HIE Access Matrix will serve as a guide that allows participating organizations the ability to establish HIE access levels for authorized users within their organization.

4. The HIE Access Matrix must be used by the state designated HIE to assign staff (i.e., staff of the state designated HIE and staff of Business Associates) to the level of access that ensures that only minimum necessary access to the statewide HIE is allowed. Staff access to PHI that is available through the statewide HIE is permitted as long as the individual is in good standing[3]. Staff access to PHI will be granted for the daily operations and maintenance of the statewide HIE.

---

[1] A Participating Organization is any health care provider that enters into a Participation Agreement with the state designated HIE.
[2] Minimum necessary refers to the least amount of information necessary to render care.
[3] Staff in good standing are those that have not been terminated by the state designated HIE for inappropriate access of the statewide HIE as outlined in the *Suspension and Termination of User Access* policy.

5. The state designated HIE must request that participating organizations identify a system administrator within their organization. The state designated HIE will require the administrator to:

    a) Identify new and existing users within their organization to be properly registered by the organization;

    b) Assign levels of HIE access to authorized users that appropriately correspond to their role within the organization;

    c) Modify a user's HIE access level in the event that a change in role within the organization has occurred where they require a different level of access; and

    d) Immediately terminate HIE access for any user that is not in good standing, which includes resignation or termination.

6. The state designated HIE must provide technical assistance and guidance to the administrator of the participating organization in assigning access levels to appropriately authorized users. The state designated HIE must require participating organizations and Business Associates to attest to the appropriateness of the roles assigned and the corresponding level of access.

7. The state designated HIE must allow users to query the HIE in accordance with the *Consumer Choice* policy. The state designated HIE is responsible for maintaining the integrity of roles assigned, via the HIE Access Matrix, in the core infrastructure of the statewide HIE.

Procedure:

The state designated HIE should implement procedures that are inclusive of the following items:

HIE Access Matrix Development, Review, and Revision

1. The HIE Access Matrix should have a column for each access level and a row for each use case (e.g., electronic eligibility, clinical lab ordering/results delivery, electronic prescribing, medication history, clinical summary exchange, etc.) and corresponding associated data, including identified sensitive health information. See *Figure 1* for a generic template.

Use Case (UC)	Associated Data (AD)	Access Level 1	Access Level 2	Access Level 3	Access Level 4	Access Level 5
UC 1	AD 1	x	x	x	x	x
	AD 2	x	x	x	x	x
	AD 3	x	x	x	x	x
UC 2	AD 1		x	x	x	x
	AD 2		x	x	x	x
	AD 3		x	x	x	x
UC 3	AD 1			x	x	x
	AD 2			x	x	x
	AD 3			x	x	x
UC 4	AD 1				x	x
	AD 2				x	x
	AD 3				x	x
UC 5	AD 1					x
	AD 2					x
	AD 3					x

Figure 1

2. The HIE Access Matrix should be developed prior to the assignment of access to users and prior to allowing access to information.

Assignment and Changes HIE Access Levels

1. The state designated HIE should provide consultation to an administrator prior to any initial identification and assignment of access levels to users, which will include at a minimum:

    a. A detailed explanation of the HIE Access Matrix; and

    b. Recommendations as to what levels of access will most adequately correspond with the current roles of an identified user.

2. Identified access levels for users should be operationalized within one (1) business day of receipt of the request by the state designated HIE.

3. The state designated HIE should require the administrator to terminate a user's access immediately in the event that the user resigns from the organization or is terminated.

Associated Policies:

1. *Audit*
2. *Consumer Choice*
3. *Enforcement*
4. *Suspension and Termination of Provider Access*
5. *Sensitive Health Information*
6. *User Authentication*
7. *User Authorization*

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange

USER AUTHORIZATION	
Approval Date: *11-09-10*	Scheduled Review Date: *11-09-11*

Goal: The *User Authorization* policy aims to assure the confidentiality of health information by requiring the state designated health information exchange (HIE) to establish user access levels. Authorization levels are necessary to appropriately determine what information is available to users accessing the statewide HIE.

Purpose: This policy describes the responsibility of the state designated HIE to define the requirements for establishing user access, and ensuring that users are properly authenticated. Users must be authorized to access information through the statewide HIE that is consistent with the job functions as determined by the participating organization. User authorization is critical to establishing user accountability and managing risk.

Policy:

1. The state designated HIE must require participating organizations to quarterly audit their user accounts. These audits must review what information was accessed as compared to the care that was provided by the user.

2. The state designated HIE must require participating organizations to validate that consumer assent has been obtained prior to querying the statewide HIE. The state designated HIE needs to require participating organizations to have a robust policy around assent to query consumer information through the statewide HIE.

3. The state designated HIE must audit for break the glass activity and review findings with the participating organizations. As part of the review process, the state designated HIE must investigate to determine if participating organizations are appropriately using their emergency access privileges.

4. The statewide HIE must require participating organizations to notify consumers on a timely basis when authorized individuals inappropriately access consumer information. Participating organizations will need to take immediate corrective action against users that violate their privileges.

Procedure:

The state designated HIE should implement procedures that are inclusive of the following items:

1. The state designated HIE should protect against unauthorized use by requiring participating organizations to audit their authorization records on a quarterly basis. Participating organizations should also be required to report unauthorized access, use, and disclosure to the consumer within (10) ten days of discovery.

2. The state designated HIE should require participating organizations to validate consumer assent to access their information through the statewide HIE. As part of the registration process, participating organizations should be required to affirm that this process has occurred through a notation in the file of an electronic flag.

3. The state designated HIE should require participating organizations to take appropriate corrective action against users that inappropriately access information through the statewide HIE. Suspension and terminations should be subject to an appeal process.

Associated Policies:

1. *Audit*
2. *User Authentication*
3. *Enforcement*
4. *Notification of Breach*
5. *Participating Organization Access*

The MARYLAND
HEALTH CARE COMMISSION

Statewide Health Information Exchange

USER AUTHENTICATION	
Approval Date: *01-11-11*	Scheduled Review Date: *01-11-12*

Goal: The *User Authentication* policy aims to protect patient information by ensuring that verification of a user's identity occurs before access is granted; preventing unauthorized users from accessing the statewide health information exchange (HIE). User authentication is an essential component for maintaining the integrity of protected health information (PHI). The ultimate objective is to achieve two factor authentication. Stakeholders must be assured that information available through the statewide HIE is accessed by only those individuals that have a legitimate need to access the information.

Purpose: This policy describes the state designated HIE's responsibilities as it relates to authenticating users to the HIE. User authentication is critical to ensuring that the individual attempting to access the statewide HIE is who they claim to be. Authentication also substantiates that the user is permitted to access information within the statewide HIE.

Policy:

1. The state designated HIE must authenticate users accessing the statewide HIE on a direct basis and require participating organizations to authenticate users accessing the statewide HIE prior to granting them access. Authentication enables the state designated HIE to validate that users attempting to access the HIE are who they claim to be. Authentication must occur at each attempt the user tries to access the statewide HIE.

2. The state designated HIE will authenticate users accessing the statewide HIE and require participating organizations to authenticate users accessing the statewide HIE using the following matrix:

User Connectivity	Authenticating Party	Required Authentication Protocol			
		Single Factor[1]	Single Factor w/ Two Factor Characteristics[2]	Two Factor[3]	Multi-Factor
Providers					
a. Direct via the HIE provider portal	State Designated HIE		✓		
b. Through an EHR system onsite of a Participating Organization	Participating Organization		✓		
c. Through an EHR system remote from a Participating Organization	Participating Organization		✓		
Consumers					
d. Direct via the HIE consumer portal	State Designated HIE	[TBD]			

[1] Single factor authentication includes a user name and strong password.
[2] Two factor characteristics include user name and password with an additional security precaution, such as one or more security questions, device registration, etc.
[3] Two factor authentication includes a user name, password and secret key, private key, one-time password, token, etc. (Examples include, SecurID, IronKey, PhoneFactor, and Virtual Token™ multi-factor authentication, etc.)

3. The state designated HIE must accept the credentials of users accessing the statewide HIE through a third party EHR. User credentials may only be accepted by the state designated HIE after a user has gone through appropriate registration and identity proofing procedures of the state designated HIE.

4. The state designated HIE will, at a minimum, follow the National Institute of Standards and Technology (NIST) Level 2 registration as outlined in the most recent version of *Special Publication 800-63: Electronic Authentication Guideline*. The state designated HIE must also follow the registration record retention requirements for Level 2.

5. The state designated HIE must require participating organizations to ensure that each user is assigned a unique user name and password. Individual unique user names and passwords must be established in accordance with the most recent version of the NIST, Special Publication 800-63: *Electronic Authentication Guideline*. The state designated HIE must use the protocols established by NIST in requiring that all participating organizations adopt these standards.

6. The state designated HIE must encrypt user authentication data stored in the statewide HIE. The state designated HIE is required to use industry best practices in determining the level of encryption for user authentication data. Encryption of authentication data is required to protect the data.

7. The state designated HIE is required to periodically audit user authentication logs as part of its routine audit process. Included in the audit, the state designated HIE must develop protocols that identify outliers for the audit of the authentication and assessment logs. Any unusual findings from the audit must be investigated and resolved in a timely manner.

8. The state designated HIE will maintain an audit trail of user authentication logs for a length of time consistent with state and federal requirements. The information must be housed in a retrievable storage medium. The state designated HIE is required to perform periodic testing to demonstrate that stored data is recoverable.

Procedure:

The state designated HIE should implement procedures that are inclusive of the following items:

1. The state designated HIE should require participating organizations to use an EHR product that complies with the NIST standards for user authentication.

2. The state designated HIE should institute audit procedures that ensure that only appropriately authenticated users are granted access to the HIE and report any unusual findings back to the participating organizations.

3. The state designated HIE should require participating organizations to report any unusual findings from their authentication log audit to the state designated HIE within seventy-two (72) hours of discovery.

Associated Policies:

1. *Audit*
2. *Authorization*
3. *Consumer Access & Authentication*
4. *Enforcement*
5. *Notification of Breach*
6. *Participating Organization Access*

[Intentionally Left Blank]

Marilyn Moon, Ph.D., Chair

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

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

4160 Patterson Avenue
Baltimore, MD 21215
(410) 764-3460
www.mhcc.maryland.gov